

You have reached a collection of archived material.

The content available is no longer being updated and may no longer be applicable as a result of changes in law, regulation or our administration. If you wish to see the latest content, please visit the [current version of the site](#).

For persons with disabilities experiencing difficulty accessing content on [archive.defense.gov](#), please use the DoD Section 508 Form. In the form, please indicate the nature of your accessibility issue/problem and your contact information so we can address your issue or question.



News

[News Articles](#)
[News/Casualty Releases](#)
[Press Advisories](#)
[News Transcripts](#)
[Publications](#)
[Speeches](#)
[Contracts](#)
[Testimony](#)
[Messages](#)
[Special Reports](#)

Secretary of Defense

[Biography](#)
[Speeches](#)
[Messages](#)
[Testimony](#)
[Travel](#)
[News Photos](#)

Deputy Secretary of Defense

[Biography](#)
[Speeches](#)
[Travel](#)
[News Photos](#)

Photos/Videos

[Lead Photos](#)
[News Photos](#)
[Photo Essays](#)
[Week in Photos](#)
[Videos](#)
[DoD Video News](#)
[Imagery Archive](#)

Other

[Briefing Slides](#)
[Pentagon Press Slogos](#)
[Press/Media Queries](#)
[Military Commissions](#)
[Detainees](#)
[Other News Sources](#)

Secretary of Defense Speech

Press Operations

SPEECH

Facebook | Twitter | YouTube | LinkedIn | RSS

Business Executives for National Security (Export Control Reform)

Remarks as Delivered by Secretary of Defense Robert M. Gates, Ronald Reagan Building and International Trade Center, Washington DC, Tuesday, April 20, 2010

Thank you, General, thanks for that kind introduction. I also would like to thank my colleague Undersecretary Ellen Tauscher for being here for moral support.

And Monty thank you for your long service to our country, most recently leading the Defense Department's efforts to combat improvised explosive devices. Your efforts have saved the lives and limbs of countless men and women in uniform.

My thanks as well to Business Executives for National Security for hosting this event. In areas like accounting, procurement, privatization, and excess base structure, BENS has identified problems and proposed solutions that have saved the taxpayers billions of dollars and made our military a more effective fighting force.

As many of you know, for the better part of three years now I have spoken out at various times about the need to adapt and reform America's national-security apparatus better to deal with the realities of the post-Cold War era.

Some of those necessary shifts include:

- Enhancing America's civilian instruments of national power – above all diplomacy and development – and better integrating them with our military;
 - Rebalancing the defense establishment to reflect the lessons learned and capabilities gained from recent conflicts, especially counterinsurgency, stability, and reconstruction operations;
 - And, most recently, reforming the way we build the capacity of allies and partners to better fight alongside us and secure their own territory.
- All these institutional shifts are, to one degree or another, aimed at improving the way the United States works with and through other countries to confront shared security challenges.

So is the matter I want to discuss today: the need to reform the U.S. government's regulations and procedures for exporting weapons and so called dual-use equipment and technology.

Earlier this year, the president announced that he would seek to further enhance our national security through substantial changes to our export-control regime. He did so with the unanimous support of his entire national-security team. This afternoon I will focus on what I believe are the compelling security arguments for the changes recommended by the president.

I want to state from the outset how critically important it is to have a vigorous, comprehensive export-control system that prevents adversaries from getting access to technology or equipment that could be used against us.

The problem we face is that the current system – which has not been significantly altered since the end of the Cold War – originated and evolved in a very different era, with a very different array of concerns in mind.

As a result, its rules, organizations, and processes are not set up to deal effectively with those situations that could do us the most harm in the 21st Century – a terrorist group obtaining a critical component for a weapon of mass destruction, or a rogue state seeking advanced ballistic-missile parts. Most importantly, the current arrangement fails at the critical task of preventing harmful exports while facilitating useful ones.

The United States is thought to have one of the most stringent export regimes in the world. But stringent is not the same as effective. A number of lapses in recent years – from highly sensitive materials being exported to vital homeland security capabilities being delayed – have underscored the flaws of the current approach.

Several factors contribute to these kinds of scenarios, which at worst could lead to the wrong technology falling into the wrong hands. One major culprit is an overly broad definition of what should be subject to export classification and control. The real-world effect is to make it more difficult to focus on those items and technologies that truly need to stay in this country. Frederick the Great's famous maxim that "he who defends everything defends nothing" certainly applies to export control.

This problem goes back a long way, and was evident well before the collapse of the Soviet Union. In

SHARE

Most Recent Speeches

- 08/15/2015
Remarks at Chattanooga Memorial Service
As Delivered by Secretary of Defense Ash Carter, Chattanooga, Tennessee
- 08/14/2015
Army Chief of Staff Change of Responsibility
As Delivered by Secretary of Defense Ash Carter, Fort Myer, Virginia
- 07/31/2015
Remarks at the Military Child Education Coalition Training Seminar
As Delivered by Secretary of Defense Ash Carter, Washington, D.C.
- 07/31/2015
Remarks at Retirement Ceremony for Admiral Winnefeld
As Delivered by Secretary of Defense Ash Carter, Fort Myer, Virginia
- 07/29/2015
Statement on the Impacts of the Joint Comprehensive Plan of Action before the Senate Armed Services Committee
As Delivered by Secretary of Defense Ash Carter, Washington, D.C.
- 07/11/2015
Remarks to the National Association of Counties
As Delivered by Secretary of Defense Ash Carter, Charlotte, North Carolina
- 07/08/2015
Vietnam War Congressional Commemoration
As Delivered by Secretary of Defense Ash Carter, Washington, D.C.
- 07/07/2015
Statement on Counter-ISIL before the Senate Armed Services Committee
As Delivered by Secretary of Defense Ash Carter, Washington, D.C.
- 06/23/2015
GEINT Symposium 2015
As Delivered by Deputy Secretary of Defense Bob Work, Washington Convention Center, Washington, DC
- 06/22/2015
China Aerospace Studies Institute
As Delivered by Deputy Secretary of Defense Bob Work, RAND Corporation, Arlington, VA

1982, when I became deputy director for intelligence at CIA, my responsibilities included tracking prohibited transfers of U.S. technology. It soon became apparent that the length of the list of controlled technologies outstripped our finite intelligence monitoring capabilities and resources. It had the effect of undercutting our efforts to control the critical items. We were wasting our time and resources tracking technologies you could buy at RadioShack.

Today, the government reviews tens of thousands of license applications for export to EU and NATO countries. In well over 95 percent of these cases, we say "yes" to the export. Additionally, many parts and components of a major piece of equipment – such as a combat vehicle or aircraft – require their own export licenses. It makes little sense to use the same lengthy process to control the export of every latch, wire, and lug nut for a piece of equipment like the F-16, when we have already approved the export of the entire aircraft.

In short, the time for change is long overdue if the application of controls on key items and technologies is to have any meaning. We need a system that dispenses with the 95 percent of "easy" cases and lets us concentrate our resources on the remaining 5 percent. By doing so, we will be better able to monitor and enforce controls on technology transfers with real security implications while helping to speed the provision of equipment to allies and partners who fight alongside us in coalition operations.

A second major obstacle we face is the bureaucratic apparatus that has grown up around export control – a byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government. In theory, this provides checks and balances – the idea being that security concerns, customarily represented by DoD, would check economic interests represented by the Commerce Department and balance out diplomatic and relationship-building equities represented by State. In reality, this diffusion of authority – where separate export-control lists are maintained by different agencies – results in confusion about jurisdiction and approval, on the part of companies and government officials alike.

It creates more opportunities for mistakes, enforcement lapses, and circumvention strategies such as "forum shopping," where exporters with problematic license applications try different agencies looking for the best result. In one instance, an individual was caught intentionally exporting a controlled item without a license, but escaped prosecution by presenting two conflicting determinations from two different government agencies. The item in question was a carbon composite material used in ICBM nose cones.

As a result of this dispersed arrangement, the U.S. government spends an enormous amount of time and energy on what are essentially process questions – trying to decide which agency has jurisdiction – as opposed to the more important issue of whether a given technology can be safely exported. These internal squabbles can have real world consequences. A fight between agencies over jurisdiction, for example, delayed a program to place new screening equipment in U.S. and overseas airports.

Correspondingly, many companies face a frustrating situation where an exporter with a single purchase order may have to seek licenses from two separate agencies, and could be approved by one but denied by the other. Additionally, because it is so difficult to modify or update the control lists, a controlled item might never be considered for a lower level of restriction even if it becomes much less sensitive and important over time.

The system has the effect of discouraging exporters from approaching the process as intended. Multinational companies can move production offshore, eroding our defense industrial base, undermining our control regimes in the process, and not to mention losing American jobs. Some European satellite manufacturers even market their products as being not subject to U.S. export controls, thus drawing overseas not only potential customers, but some of the best scientists and engineers as well. At the same time, onerous and complicated restrictions too often fail to prevent weapons and technologies from going places they shouldn't. They only incentivize more creative circumvention strategies – on the part of foreign companies, as well as countries that do not have our best interests at heart.

Concurrently, we have not updated our system to deal with the U.S. military's transition to off-the-shelf procurement. More and more, our military is taking advantage of commercially manufactured items, presenting challenges when determining whether or not a given technology is acceptable for export. There are electronic components used in many third-generation cellular devices that are also important components of sophisticated stealth-defeating radar systems. We need to update our export-control system to reflect these realities.

Finally, the current export-control regime impedes the effectiveness of our closest military allies, tests their patience and goodwill, and hinders their ability to cooperate with U.S. forces – this at a time when we count on allies and partners to fight with us in places like Afghanistan and potentially elsewhere. Not too long ago, a British C-17 spent hours disabled on the ground in Australia – not because the needed part wasn't available, but because U.S. law required the Australians to seek U.S. permission before doing the repair. These are two of our very strongest allies for God's sake! Similarly, close, long-standing allies and partners like South Korea have bought U.S. aircraft only to encounter difficulties and delays in getting spare parts – something that weakens our bilateral relationships, our credibility, and ultimately American security.

That is one of the reasons why several U.S. secretaries of defense representing multiple administrations of both political parties have voiced frustration over the export-control system. As defense secretaries, we have all, at one time or another, had to sit across the table from defense ministers from important allies or new partners and explain why the U.S. government is unable to follow through expeditiously on its commitments to provide the weapons, equipment, and support they have been promised and paid for. It is not an edifying experience. All the while, other countries that do not suffer from our encumbrances are taking the opportunity to sell weapons, build relationships, and improve their strategic position and economic standing.

Some obstacles to having a strategically sound defense trade relationship can be addressed through bilateral agreements with our closest allies and partners. In 2007, the U.S. signed Defense Trade Cooperation Treaties with both the United Kingdom and Australia – treaties that still await ratification by the Senate. Through streamlined export-control arrangements and enhanced technology security measures, these agreements would substantially improve our ability to equip and support U.S., U.K., and Australian forces deploying in combat operations. They contain provisions allowing for the establishment of export-authorized groups of U.S., U.K., and Australian companies. Except for a short list of truly critical equipment and technologies, these trusted companies could largely avoid individual export licenses. I remain hopeful that the Senate will give advice and consent to both of these treaties prior to the summer recess.

The kinds of common sense changes contained in the U.K. and Australia treaties are a step in the right direction, but these two key allies. But international agreements are still no substitute for the kind

Defense.gov Secretary of Defense Speech Business Executives for National Security Export Control Reform)

of fundamental systematic reform of export control that this country urgently needs.

The fact is, for all the reasons I described earlier, America's decades-old, bureaucratically labyrinthine system does not serve our 21st-century security needs or our economic interests. It is clear our current limitations in this area undermine our ability to work with and through partners to confront shared threats and challenges – from terrorism to rogue states to rising powers. Our security interests would be far better served by a more agile, transparent, predictable, and efficient regime. Tinkering around the edges of our current system will not do.

For these reasons and more, in August of last year, the president directed a broad-based review of the U.S. export-control regime. He has called for reforms that focus controls on key technologies and items that pose the greatest national-security threat. These include items and technologies related to global terrorism, the proliferation and delivery systems of weapons of mass destruction, and advanced conventional weapons. In short, a system where higher walls are placed around fewer, more critical items.

Following this directive, and informed by a recent National Intelligence Council assessment of the key national-security considerations, I have worked closely with my counterparts at the departments of State, Commerce, Homeland Security, as well as with the director of national intelligence and the national security advisor to develop a blueprint for such a system. Our plan relies on four key reforms: a single export-control list, a single licensing agency, a single enforcement-coordination agency, and a single information-technology system.

First, a single export-control list will make it clear to U.S. companies which items require licenses for export and which do not. This single list, combined with a single licensing agency, would allow us to concentrate on controlling those critical technologies and items – the “Crown Jewels” if you will – that are the basis for maintaining our military technology advantage, especially technologies and items that no foreign company or government can duplicate. Items that have no significant military impact, or that use widely available technology, could be approved for export quickly. We envision a more dynamic, tiered control system where an item or technology would be “cascaded” from a higher to a lower level of control as its sensitivity decreases.

Second, a single licensing entity, which will have jurisdiction over both munitions and dual-use items and technologies, will streamline the review process and ensure that export decisions are consistent and made on the real capabilities of the technology. This single entity would also reduce exporters' current confusion over where and how to submit export-license applications, as well as which technologies and items are likely to be approved. The administration is currently preparing options for the agency's location, and I anticipate a presidential decision later this spring.

Third, the coordination of our currently dispersed enforcement resources by one agency will do a great deal to strengthen enforcement, particularly abroad, as well as coordination with the intelligence community. Those who endanger our troops and compromise our national security will not be able to hide behind jurisdictional uncertainties or game the system. Violators will be subject to thorough investigation, prosecution, and punishment severe enough to deter lawbreaking.

Fourth, a single, unified informational technology infrastructure will reduce the redundancies, incompatibilities, and waste of taxpayer money that our current system of multiple databases produces. For example, a single online location and database would receive, process, and help screen new license applications and end-users.

Of course, the question of which end-users are eligible to receive our technology is a critical national-security concern. An essential component of the reformed system is the list of entities – terrorist organizations, rogue states, and others – that cannot be allowed access to sensitive items. This would deny them technology or force them to acquire it through more difficult routes. In order to facilitate compliance and tracking, we propose to consolidate current lists of banned end-users into one single frequently-updated list that will be easy for those performing transfers to consult. Entities can be added at any time if there is reasonable cause to believe they are involved in activities contrary to U.S. national-security interests.

These fundamental reforms, if enacted together, will improve America's ability to work with and fight alongside allies and partners by setting clear, transparent standards – standards that will make it possible to share technology more freely, especially items needed and used by all of us to counter common threats. I'd like to emphasize that the new system will be in full compliance with all of our existing multilateral treaties and obligations. The prospect of more defense trade with the U.S. will incentivize other nations to strengthen their own export regimes. Given how quickly and how easily goods and information now can flow around the world, export controls are far more effective when they involve multiple partners with shared interests and values.

As happens with any major reform to an entrenched, long-standing system, there will be resistance and criticism. Some people will be concerned that having fewer items subject to the most onerous export restrictions will make it easier for hostile states or groups to obtain weaponry and technology that potentially could be used against us. No system – above all, the current one – is foolproof. But by consolidating most export licensing functions in one agency and creating an enforcement coordination agency, we can focus our energies and scrutiny on technologies that truly could threaten American security, making it is far less likely that these critical items will fall into the wrong hands. It is also important to bear in mind that the U.S. government will retain the ability to impose economic sanctions on any foreign country or group, to include prohibiting the export of ANY equipment, material, or technologies that could have military use.

We will turn these principles and proposals into action through a three-phased process that will unfold over the course of the next year. In the first phase, the executive branch begins the transition towards the single list and single licensing agency by making significant improvements to the current system. These efforts would include establishing criteria for a tiered control list and standing up an integrated enforcement center. The second phase would complete the transition to a single IT structure, implement the tiered control list, and make substantial progress towards a single licensing system.

These changes, which can be made through executive action, represent substantial progress and momentum towards reform. But they are by themselves insufficient to fully meet the challenge at hand. We need a final, third phase – a thorough overhaul of the current system along the lines I have described today, most notably the single licensing agency and single enforcement coordination agency. These fundamental changes will require congressional action.

I greatly appreciated the chance to meet earlier with a number of senior members of Congress this year to discuss this topic. I valued the feedback and suggestions they provided at the time, and I look forward to further dialogue. It's the president's hope that his national-security team can continue to work closely with Congress and all of the key committees to turn these proposals into legislation that the

president can sign sometime this year.

I know better than most that earlier attempts at reform have foundered in the face of resistance. The proposition that a more focused and streamlined system actually helps our national security can go against conventional wisdom. But for the reasons I've described today, I believe it is the right approach, and it is urgently needed given the harmful effects of continuing with the existing set of outdated processes, institutions, and assumptions.

Indeed, America's ability to engage effectively with the rest of the world and keep our most sensitive technology away from those who would do us harm depend critically on our ability to get this right. I look forward to working with the Congress and my interagency colleagues to achieve the kind of systematic reform that will benefit both the security and prosperity of the American people. Thank you.

0 ?? ?? 0 0 1

- Home

Today in DOD

About DOD

Top issues

News

Photos/Videos

DoD Sites

Contact Us

Resources
- Inspector General

Privacy & Security

Link Disclaimer

Recovery Act

FOIA

USA.gov

No FEAR Act

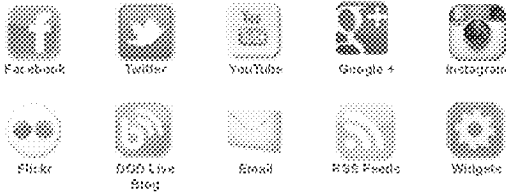
Plain Writing Act of 2010

Accessibility/Section 508
- Join the Military

Careers

Web Policy

STAY CONNECTED



MORE SOCIAL MEDIA SITES »

**The Administration's Export Control Reform Plans
Remarks by General Jones, National Security Advisor
June 30, 2010**

Introduction

Thank you for your kind introduction. I also want to extend my thanks to Senator Murray and Senator Bond for their leadership in the creation of the Senate Aerospace Caucus. It is an excellent means of ensuring that our aerospace industry remains strong and agile and viable, given how critical it is to our national and economic security. And thank you to Marion Blakey as well for all the work that you and your team have done in helping organize this event. I also want to extend a warm welcome to our Canadian colleagues.

I appreciate the opportunity to talk with you today about the President's export control reform initiative, building on Secretary Gates' comments in April and the brief overview that Secretary Donley provided at your inaugural meeting in May.

Export controls are a critical tool in our national defense, and, more specifically, our non-proliferation efforts. Our national security requirements in the 21st century include a much broader array of factors than in the past. Our economic security is part of our national security. The future of the United States' national security in the 21st century is our competitiveness. Export controls have a far-reaching impact on our broader national security interests, as they affect the health and competitiveness of our industrial base and our interoperability with our allies. Most significantly, they enhance our ability to provide our men and women in uniform with the best tools possible, while ensuring that those tools do not find their way into the hands of the adversaries they may face.

Yet, despite their importance, export controls have not received the sustained high-level attention they deserve, and as a result, our export control system has not changed to meet the new requirements of a changed world. Export control reform is a unique issue where there is unanimous interagency agreement. The United States has one of the most stringent export control systems in the world. But as Secretary Gates said, being stringent is not the same as being effective. Our system was designed during the Cold War for a bi-polar world that no longer exists, with a very different economy from the one we have today. For its time, the system worked well, based on some fundamental assumptions:

- Weapons development was done by a limited community of dedicated people and companies that could be identified easily and effectively controlled.
- Weapon systems were exported as finished products, and in some cases we specifically created lower technology “export versions” of weapons systems that we initially never intended to sell.
- “Specifically designed for military use” – a term still used in our munitions controls today – meant what it says: items were intended only for military use having little or no civilian use.
- Commercial systems with possible military use were readily distinguishable from items specifically designed for military use.

- Advanced technologies were developed for the military, and only later did they find their way into commercial applications. Now, in many instances, the reverse is true.
- There was little if any reason to export any of these technologies or systems to embargoed countries.

Based on the realities of that time, our export control system developed into three different systems – one for munitions, that is, military, items administered by the State Department, another for commercial items that had possible military uses administered by the Commerce Department, and a yet another for embargoed items administered by the Treasury Department.

But, as we all know, there have been tremendous political, economic, and military change since our current structures were established:

- We live in a 21st century multi-polar world.
- Industries and competition are now global.
- Shrinking defense budgets and the high cost of individual weapons systems often make procuring only for our own use insufficient to support the development, design and production costs.

- Advanced technology development trends have almost completely reversed – now they are predominantly from the commercial sector. This reality is reflected in our military’s commercial-off-the-shelf procurement policies.
- Our existing embargos now have some exceptions for certain technological exports that advance U.S. interests. For example, certain Internet software applications to facilitate the free flow of information and also civil aircraft parts and components for commercial safety-of-flight.
- The Cold War ended, and with it, the block structure of the West versus East that permitted us to develop the consensus that the previous export control systems work against the Eastern Block.

The bottom-line is that the world has changed dramatically. Procurement patterns have changed, markets have changed, the threats we face are different, and the economy is global. What has not changed, however, is the basic structure and premise of our export control process. We have made improvements over the years, particularly in working with our trading partners in the multilateral export control regimes, but those changes have been patch-work, with tailor-made fixes to address specific problems, rather than being the result of a more holistic and coordinated approach to our entire system. As a result, our system today is made up of a number of antiquated systems cobbled together over time, leaving us with a seriously fractured overall approach to export controls.

We should be striving for a system that prevents harmful exports while facilitating useful ones. Our current system is not meeting that objective. In fact, our system itself poses a potential national security risk based on the fact that its structure is

overly complicated, contains too many redundancies, and tries to protect too much. In short, we are hard to work with. As Secretary Gates has often said, we need to have a “higher fence around a smaller yard.”

Our approach to reform reflects the realities of our current system. We have:

- Two different control lists with fundamentally different structures, administered by two different departments;
- Three different primary licensing agencies, none of which sees the others’ licenses, and each of which has unique procedures and, significantly, their own unique definitions for the same terms;
- A multitude of enforcement agencies with overlapping and duplicative authorities; and
- A number of separate information technology (IT) systems, none of which are accessible to or easily compatible with the other. In fact, we have one licensing agency with no IT system that can receive license applications or issue licenses.

This Administration has determined that we need fundamental reform in all four of these areas. Details of this decision were announced by Secretary Gates in a speech on April 20, when he outlined the Administration’s three-phase implementation plan, covering all four of these areas, to accomplish reform for our national security.

Phases I and II will result in fundamental reform of our system while maintaining our current interagency structure. We have assessed that we can do virtually all these items via Executive action, with some legislative changes we would like to make in the enforcement area. We are doing all of this work in close consultation with Congress. Our Phase I and II actions also establish the necessary framework for Phase III, when we would deploy the following “Four Singularities:”

- A Single Control List;
- A Single Licensing Agency;
- A Single Enforcement Coordination Agency; and
- A Single IT system.

Phase III will require legislation. We have not had comprehensive export control legislation in over 30 years. We need a partnership with Congress to get this done.

I want to talk today about our plans across the three phases, highlighting some specific actions that we have taken or have in-process in Phases I and II of our implementation plan.

Implementation Plans

Control Lists – There is growing friction between our two control lists, the U.S. Munitions List and the Commerce Control List. This is because the lists are still

designed to address the Cold War-era assumptions I mentioned earlier, when technologies were developed first for the military and only later converted to commercial applications. That is no longer true, but these assumptions remain as the underlying basis of our control lists. As a result, jurisdictional disputes involving the two lists have diverted attention from the more important issue of whether an item should be controlled and how.

I issued new commodity jurisdiction guidelines to the departments in June of last year, which was a step in the right direction, but we need to do much more.

Getting the control lists right has been our highest priority in Phase I, as everything else flows from what we control. This is also the most challenging area, so we have addressed it first.

In Phase I we have developed independent objective criteria to create a tiered control list structure, with the “crown jewels” and WMD in the top tier and then cascading down the tiers as the technology or product life cycle matures. This approach has several clear advantages:

- First, it will ensure that we have a way to quickly add new items and technologies, as appropriate, but equally important, will also provide a means for eventually removing items from our lists as technologies age and are no longer in need of being controlled. You may be surprised to learn that, as part of our review, we uncovered a copy of the very first Munitions List, dated 1935, that includes military railway trains. What may surprise you even more is that these trains remain on the Munitions List today.

- Second, it will help us to prioritize our controls, with the most stringent controls on the highest tier items and more flexible licensing mechanisms in the lower tiers, to include program licenses, a type of license I know is of great interest to the aerospace community. Currently a bracket or screw used in an F-18 is treated the same for control purposes as the aircraft itself. I think we can all agree that an advance fighter jet poses a much higher threat than a screw that is merely cut to a specific length.
- Third, it will help us prioritize how we process license applications. All items are not equal, yet our current licensing processes are very much like a production line, each license application processed in the order it is received. The tier of control will help us determine how we process a license application. For example, fingerprinting ink controlled to prevent human rights abuses should not receive the same interagency technical review as something like a five-axis machine tool.

We have devoted considerable time and effort to developing the tiering criteria over the last five months, and after several rounds of tests, we have a set of criteria to use in this process. The criteria may well change again as we get more into the list reform process. But the tiering criteria will not resolve the current jurisdictional problems between the two lists, which is another important Phase I action item.

The jurisdictional problem is exacerbated by the completely different structures of our two lists – the Commerce List is generally a positive list, which means that an item is only controlled if it is on the list. For each item on the list, the Commerce List contains detailed technical parameters that are used by exporters to determine

if their items are controlled. Most of the Munitions List, however, is not a positive list. Instead, it is based on broad general descriptions, which results in capturing every nut, bolt and screw of a munitions item. The lack of specificity, the continued use of the “specifically designed for military use” standard, and the reality that our military has transitioned to more commercial-off-the-shelf procurement, has made the jurisdictional problem a major one that needs to be resolved.

That is why we have developed what we call the jurisdictional “bright line process” for identifying whether items are on the Munitions List or on the Commerce List. With the basic criteria for the tiers and the bright line process now in place, we have moved into Phase II for the control lists.

We currently have technical experts applying both the criteria and bright line process to an entire category on the Munitions List, together with the related entries on the Commerce List. At the end of this work, we will have a positive list for that category, an end of jurisdictional uncertainty, and the process begun to restructure both lists into identical structures. We will use the results of this first category to make adjustments as necessary and then move more aggressively to the rest of the lists.

One of the core issues in current interagency jurisdictional disputes is the view that items that may not be munitions items should still be controlled on the Munitions List to ensure a sufficient level of control, if there is no existing entry on the Commerce List to which the item can be added. We are resolving this problem by implementing a recommendation from AIA – the creation of “holding” entries on the Commerce List. We will be able to place items into these control entries if we

decide that they should be controlled but are not munitions items and do not otherwise fit into an existing entry on the Commerce List.

This effort will also help us determine the volume of Congressional notifications that may be necessary. There is a statutory process for notifying Congress before removing items from the Munitions List, whether we intend to decontrol items or move them to the Commerce List. We have discussed the process with oversight committee staff and are committed to work with them, so they can advise us on the best means of handling the notifications.

This entire process will prompt us to develop a series of proposals to the multilateral export control regimes, to add, update, or remove controls, as the most effective controls are those that are multilateral.

By the end of Phase II, we will have two control lists in the same structure that are more focused on key items and technologies predominantly subject to multilateral controls and that are clear and easily updated and more easily enforced.

Licensing: As I mentioned earlier, we currently have 3 primary licensing agencies, none of which sees the others licenses. They use different procedures, have different regulations, and different definitions for the same terms. As a result of this stove-piped approach, the U.S. Government has no means of knowing what it has collectively authorized to a foreign company or government and, more significantly, what we have denied.

To resolve this, in Phase I we are identifying practices, business processes, and definitions, with the aim of making changes that will harmonize how we do

business and remove inherent discrepancies and contradictions between the current systems. One item on which we have made significant progress is the development of a single application form that would be used by all three licensing agencies. While this may seem mundane, it will be a significant improvement for U.S. exporters and an important early step in developing our single IT system.

Last Friday we published our first encryption reform regulation which the President mentioned in his March 11 speech at the Export Import Bank. The revised rule enhances our national security by allowing the government to focus its resources on the more sensitive encryption items, while cutting the red tape by eliminating the review of readily available encryption items, like cell phones and household appliances. The other regulation change that the President mentioned on dual- and third-country nationals will be published soon.

In Phase II, we will deploy changes in all of these areas and further align the systems by putting in place licensing policies linked to the new control list tiers. By the end of Phase II, we will see a complete transition to standardized licensing systems based on the two mirrored control lists that will result in more timely, transparent and predictable processes.

Enforcement: There are a number of enforcement agencies with overlapping and duplicative authorities, with Homeland Security (ICE) and Justice (FBI) having authority to investigate violations of all three primary licensing agencies' regulations and Commerce having authority to investigate violations of the dual-use licensing system. There is duplication of resources and insufficient coordination of enforcement investigations. We have seen cases where one agency

has initiated an investigation, only to spoil an undercover operation by another agency.

In Phase I, we are in the process of standing up what we call the Export Enforcement Fusion Center, a permanent standing office staffed by employees from all of the export enforcement entities and the intelligence community. This center will coordinate and de-conflict investigations, serve as a central point of contact for coordinating export control enforcement with Intelligence Community activities, and synchronize overlapping outreach programs. As the single licensing IT system comes on-line, which I will discuss in a moment, the Fusion Center will also screen all license applications, a function only currently performed comprehensively by enforcement officials for Commerce-processed license applications, which account for only 16 percent of all license applications.

This is another area in which considerable work has been done, mapping out the terms of reference that are being used to prepare an Executive Order to formally create the center.

It is in the enforcement area where we have identified some legislative changes we would like to make. We have worked together with Congress on these possible changes, which have been included in the Iran sanctions legislation. Our reform provision toughens our enforcement authorities by doing three things:

- First, it harmonizes the different maximum export control criminal penalties across four different statutes to the maximum.

- Second, it adds a civil penalty provision to one of the statutes that has none, the United Nations Participation Act, which will enhance the enforceability of certain Treasury regulations; and
- Third, it commissions a study to be conducted by the U.S. Sentencing Commission on the impact and advisability of imposing a mandatory minimum criminal sentence for export control violations, with the intent of assessing why criminal sentences for export control violations appear to be low even though these violations may impair our national security.

We appreciate our Congressional partners' collaboration with us to improve our export enforcement tools, which is important feature of the "higher fences" that Secretary Gates has referenced.

In Phase II, we will harmonize our enforcement outreach, license compliance, and inspection programs, as well as our administrative enforcement procedures and self-disclosure processes. By the end of this phase, we will have a harmonized government-wide export enforcement program that will be more capable of enforcing our controls.

IT System: Finally, an effective, integrated IT infrastructure is an essential enabler of any robust export control system. But we currently have a number of IT systems across the licensing and enforcement agencies. This fuels the problem I already mentioned about our stove-piped licensing processes, in which the U.S. Government has no way of knowing what it has collectively authorized or denied for export to any specific end-user. This increases the risk that wrong decisions can be made.

In Phase I, we have already completed an initial review to migrate the licensing agencies to USXPorts (“U.S. Exports”), a Department of Defense system that was deployed in 2003. As a first step, the State Department’s munitions licensing organization is already in the process of migrating. Follow-on steps will migrate Commerce and Treasury and the other departments and agencies that participate in the interagency review of license applications.

We are also standing up a review to build a single interface for exporters to use, rather than the two different electronic systems maintained by Commerce and State, and the paper process used by Treasury. Our IT experts are already at work with our licensing team, which is developing the single application form.

In Phase II, all the licensing agencies will migrate to a single system. For the first time, they will be able to query the system and see the universe of what is considered for export to a given end-user. In Phase II, an assessment will be initiated to determine how to integrate the single licensing system with the various enforcement systems.

By the end of Phase II in all four areas, we will have a fundamentally new system in place based on the current interagency structure – two mirrored control lists that are more tightly focused on those key items and technologies that should be protected, with harmonized business practices, policies, and definitions across our licensing and enforcement agencies, with stronger enforcement authorities, and a single IT licensing system structure.

This leads me to Phase III, where we propose transitioning our reformed system to a new interagency structure. In Phase III our goal is to:

- Merge the two mirrored lists into one;
- Merge the licensing agencies, with harmonized business practices and policies, into a single licensing agency;
- Combine Commerce's Export Enforcement office and DHS/ICE Counter-Proliferation Program into a single dedicated export enforcement unit; and
- Deploy an enterprise-wide IT system, so that we can track an export from the filing of a license application until the item leaves the port.

The Administration in recent weeks made some key decisions on its vision for Phase III. For the Single Licensing Agency, as we're calling it, the Administration supports the creation of an independent entity, governed by a Board of Directors comprised of the Cabinet officials of the current departments with export control responsibilities, which reports to the President. We anticipate that leadership of the SLA would be nominated by the President, with the advice and consent of the Senate.

For the consolidation of certain enforcement functions, it supports merging Commerce's Export Enforcement office and ICE's Counter-Proliferation Program into a single dedicated export enforcement unit within ICE. We look forward to working with the Congress on the details of our proposals and consider options for Phase III legislation.

Conclusion

These consolidations are a natural progression of our comprehensive export control reform plan. We have an aggressive agenda with an even more aggressive timetable, as our goal is to achieve Phases I and II, and seek legislation for Phase III this year. To do so, it is critical that the leaders in the Administration, the Congress, and industry work together to make it happen. Reforming our export control system is critical to our national security, to effective political-military engagement with partner nations around the world, and to America's economic competitiveness in a global and rapidly evolving economy.

At the end of this process, with your help, we hope to have a fundamentally new system, a system defined by flexibility, transparency, and predictability, and which improves the ability of exporters to comply and for the government to enforce.

Thank you for your time this afternoon and for the support that many of you and your organizations continue to provide to our efforts.

The White House

Office of the Press Secretary

For Immediate Release

August 30, 2010

President Obama Lays the Foundation for a New Export Control System To Strengthen National Security and the Competitiveness of Key U.S. Manufacturing and Technology Sectors

Tomorrow, President Obama will announce a major step forward in the Administration's efforts to fundamentally reform the export control system and will outline the foundation of our new export control system. These changes – in what we control, how we control it, how we enforce those controls and how we manage our controls – will help strengthen our national security by focusing our efforts on controlling the most critical products and technologies and by enhancing the competitiveness of key U.S. manufacturing and technology sectors.

Last August, the President directed a broad-based interagency review of the U.S. export control system with the goal of strengthening national security and the competitiveness of key U.S. manufacturing and technology sectors by focusing on current threats and adapting to the changing economic and technological landscape. The review determined that the current export control system is overly complicated, contains too many redundancies, and, in trying to protect too much, diminishes our ability to focus our efforts on the most critical national security priorities:

- The current system operates under two different control lists with fundamentally different approaches to defining controlled products, administered by two different departments. This has caused significant ambiguity, confusion and jurisdictional disputes, delaying clear license determinations for months and, in some cases, years;
- There are three different primary licensing agencies, each applying their own policies. None sees the others' licenses, and each operates under unique procedures and definitions, leading to gaps in the system and disparate licensing requirements for nearly identical products;
- A multitude of agencies with overlapping and duplicative authorities currently enforce our export controls, creating redundancies and jeopardizing each other's cases; and

- All these agencies operate on a number of separate information technology (IT) systems, none of which is accessible to other licensing or enforcement agencies or easily compatible with the other systems, resulting in the U.S. Government not having the capability of knowing what it has approved for export and, more significantly, what it has denied.

The Control Lists

Under the approach outlined by the President, agencies will apply new criteria for determining what items need to be controlled and a common set of policies for determining when an export license is required. The control list criteria are based on transparent rules, which will reduce the uncertainty faced by our Allies, U.S. industry and its foreign partners, and will allow the government to erect higher walls around the most sensitive items in order to enhance national security.

Agencies will apply the criteria and revise the lists of munitions and dual use items that are controlled for export so that they:

- are "tiered" to distinguish the types of items that should be subject to stricter or more permissive levels of control for different destinations, end-uses, and end-users,
- create a "bright line" between the two current control lists to clarify jurisdictional determinations and reduce government and industry uncertainty about whether particular items are subject to the control of the State Department or the Commerce Department, and
- are structurally aligned so that they potentially can be combined into a single list of controlled items.

To accomplish these tasks, both the U.S. Munitions List and the Commerce Control List need to be fully structured as "positive lists." A "positive list" is a list that describes controlled items using objective criteria (e.g., technical parameters such as horsepower or microns) rather than broad, open-ended, subjective, catch-all, or design intent-based criteria. Doing this will end most, if not all, jurisdictional disputes and ambiguities that have come to define our current system.

Applying the criteria, the existing two lists will be split into three tiers:

- Items in the highest tier are those that provide a critical military or intelligence advantage to the United States and are available almost exclusively from the United States, or items that are a weapon of mass destruction.
- Items in the middle tier are those that provide a substantial military or intelligence advantage to the United States and are available almost exclusively from our multilateral partners and Allies.
- Items in the lowest tier are those that provide a significant military or intelligence advantage but are available more broadly.

This flexible construct will improve the nation's national security and permit the government to adjust controls in a timely manner over a product's life cycle in order to keep lists targeted and up-to-date based on the maturity and sensitivity of an item.

Licensing Policies

Once a controlled item is placed into a tier, a corresponding licensing policy will be assigned to it to focus agency reviews on the most sensitive items:

- A license will generally be required for items in the highest tier to all destinations. Many of the items in the second tier will be authorized for export to multilateral partners and Allies under license exemptions or general authorizations. For less sensitive items, a license will not be required more broadly.
- For items authorized to be exported without licenses, there will be new controls imposed on the re-export of those items to prevent their diversion to unauthorized destinations.
- At the same time, the U.S. Government will continue our sanctions programs directed toward specific countries, such as Iran and Cuba.

The restructuring of the control lists and the harmonized licensing policies based on the tier of control will revolutionize our current control system. The preliminary results of deploying this new system highlight this fact.

- Technical experts across the government have completed the overhaul of one category of controls on the U.S. Munitions List and the corresponding entries on the Commerce Control List and have restructured USML Category VII (Tanks and Military Vehicles) into a positive, tiered list.
- The results are significant. Our preliminary analysis is that about 74 percent of the 12,000 items we licensed last year in this Munitions List category will either be moved to the Commerce Control List or will be decontrolled altogether.
- Our preliminary estimate is that about 32 percent of the total may be decontrolled altogether. Of the 26 percent of items that remain on the Munitions List, none were found to be in the highest tier of control, about 18 percent are in the middle tier, and the remaining 8 percent in the lowest tier.

Under the current system, whether a product requires a license depends on which list it falls. The same product may be subject to two significantly different licensing requirements, depending on how it is categorized.

- Examples include brake pads for the M1A1 tank. These brake pads are virtually identical to brake pads for fire trucks but the tank brake pads require a license to be exported to any country around the world, while the fire truck brake pads can be exported to virtually all countries without a

license. Still, under our current system, we devote the same resources to protecting the brake pad as we do to protecting the M1A1 tank itself.

Restructuring the control lists and applying the same licensing policies across the government will eliminate these anomalies and allow us to focus our resources on protecting the items and technologies most critical to our national security.

Export Enforcement

Agencies will focus and strengthen our enforcement efforts, including by building higher walls around the most sensitive items. There will be additional end-use assurances against diversion from foreign consignees, increased outreach and on-site visits domestically and abroad, and enhanced compliance and enforcement.

- The President will announce tomorrow that he will sign an executive order establishing an Export Enforcement Coordination Center that will coordinate and strengthen the U.S. Government's enforcement efforts – and eliminate gaps and duplication – across all relevant departments and agencies.

Information Technology Systems

Finally, the U.S. Government is transitioning to a single information technology (IT) system to administer its export control system. The Departments of State and Defense are currently being linked to the same IT system and the Department of Commerce will integrate into this system by next year. All relevant departments and agencies will have access to the system. These improvements will create efficiencies within the U.S. Government for reviewing applications and ensure that decisions are fully informed. It will also make it easier for exporters seeking licenses and for enforcement authorities to see what actions have been taken.

The Administration's goal is to begin issuing proposed revisions to the control lists and licensing policies later this year. These changes, along with enhancements to enforcement capabilities and information technology systems, will create an export control system that is more effective, transparent and predictable – one that enhances U.S. national security, improves the functioning of the government, and maintains the competitiveness of critical manufacturing and technology sectors.

As we implement these steps, the Administration will continue to work with Congress and the export control community, including on the necessary authorities to consolidate these activities under a single licensing agency and single export enforcement coordination agency.

Additive Manufacturing Symposium: The State of the Industry

Monday, February 24, 2014
Unclassified Morning Session
HST Room 1406

U.S. Department of State
P.M. Bureau
Defense Directory for Trade Controls
Defense Trade Controls Policy

Morning Agenda:

- | | |
|---|---------------------|
| 1. <i>Welcome Remarks</i> | 9:00 AM – 9:05 AM |
| PM/DDTC Deputy Assistant Secretary Kenneth Handelman | |
| ISN/NNCP Principal Deputy Assistant Secretary Vann Van Diepen | |
| 2. Tim Caffrey, Wohlers Associates | 9:05 AM – 10:00 AM |
| 3. Steve Rengers, G.E. Aviation, U.S. | 10:00 AM – 11:00 AM |
| 4. Christopher Spadaccini, Lawrence Livermore National Laboratory | 11:00 AM – 12:00 PM |
| 5. <i>Closing Remarks:</i> | 12:00 PM – 12:05 PM |
| PM/DDTC Deputy Assistant Secretary Kenneth Handelman | |

Mr. Tim Caffrey, Wohlers Associates

Tim Caffrey will set the stage for a productive morning by discussing the state of the additive manufacturing (A.M.) and the 3-D printing industry. Caffrey will address current and long term trends and developments in the field around the world. He will discuss advanced applications, growth estimates, myths associated with the technology, and what the future holds. Finally, Caffrey will address views on export control, the production of guns, and other issues related to U.S. policy.

Caffrey is a senior consultant at Wohlers Associates. His roles and responsibilities include the execution of consulting projects, public speaking, and representation of the company at national and international events. He is a principal author of the Wohlers Report, an in-depth worldwide study of the state of the A.M. and 3-D printing industry. He has worked with Wohlers Associates since 2000.

Caffrey's career in additive manufacturing began in 1992 at Boeing's Propulsion Laboratory in Seattle. There, he directed the company's first in-house A.M. facility, which grew from one system for wind tunnel models into a large operation with nine systems that provided A.M. parts throughout the corporation. In 1996, Caffrey managed the A.M. operation of Plynetics Express in Schaumburg, Illinois, which had, at the time, the largest installed base of A.M. systems in the world. He was promoted to plant manager one year later.

Caffrey's experience includes over 20 years in professional writing and editing, including maintenance procedures for Boeing aircraft, operational tests for Boeing flight testing, engine

case repair procedures at Pratt & Whitney, and advertising copywriting at Walmart's corporate headquarters. While at Boeing, he also designed flight test hardware.

Caffrey holds a Bachelor of Science in Mechanical Engineering from the University of New Mexico. He and his wife Joy live in Fayetteville, Arkansas, and have three grown children.

Mr. Steve Rengers, General Electric Aviation, U.S.

General Electric is leading the charge of bringing metal additive manufacturing into mainstream manufacturing in North America. GE Aviation is investing heavily in equipment, personnel, and facilities to internalize and advance DMLM [Direct Metal Laser Melting], a metal powder bed technology capable of producing excellent detail resolution for complex geometries and super-alloy assemblies directly from CAD files without requiring tooling. While these laser driven technologies have been around since the mid 90's, the technology utilized for aerospace applications did not emerge until 2005.

Steve Rengers' presentation will detail the research and development activities currently pursued and briefly outline the production game plan for GE's new LEAP engine fuel nozzle, which is currently slated to be the first component in large scale production. The information provided will garner insight into the primary benefits of A.M. in the eyes of one of the world's foremost manufacturing companies. Attendees will also walk away understanding Aviation's top concerns and risks associated with DMLM in America. These challenges include intellectual property and the USPTO, counterfeit parts, domestic equipment providers, and high volume supply chains. While there is much work to complete, GE has and will continue to devote top level resources to make metal additive manufacturing work.

Rengers leads the Research and Development team tasked with advancing additive technologies – equipment, materials, and processes – at the GE Additive Development Center (formerly Morris Technologies, Inc.) in Cincinnati, Ohio. Steve joined Morris Technologies in 2005 and contributed significantly to MTI's substantial growth in size and capabilities. His responsibilities included managing sales, off-site contract services, and additive manufacturing in both plastics/polymers and metals, as well as tight-tolerance CNC machining: turning, milling, and EDM. Steve is an industrial engineering graduate from the University of Cincinnati and obtained a master of business administration from Xavier University. Prior to joining Morris Technologies, Steve's career included multiple roles in manufacturing engineering and production management over the course of 10 years with a Fortune 1000, high-volume manufacturer of electro-mechanical devices. GE Aviation acquired Morris Technologies in November 2012 and established the ADC facility.

Dr. Chris Spadaccini, Lawrence Livermore National Laboratory

Chris Spadaccini will discuss Lawrence Livermore National Laboratory's (LLNL) current work in harnessing commercial A.M. technologies and developing new additive processes combined with HPC to realize higher performance materials and more efficient manufacturing processes for NNSA and other national security applications. LLNL, in conjunction with NNSA production plant, laboratory, and university partners, is developing this promising technology, which is likely to reduce manufacturing footprint by factors of 3-50, time to product by 10x, and product cost by as much as 85%.

With respect to NNSA missions, Spadaccini will also address how A.M. can improve how we sustain the stockpile, enable options for smaller stockpiles, and provide options for recapitalization of the production complex improving its posture as a deterrent. Moreover, he will speak to how A.M. will allow us to understand the "art-of-the-possible," as well as how AM could accelerate proliferation.

Finally, Spadaccini will argue that it is imperative there be a robust programmatic initiative teaming the national laboratories with industry and academia to develop and reap the benefits afforded by A.M. for national security missions, while concurrently informing the threats it may pose.

Spadaccini is currently the Principal Investigator of several advanced materials and additive manufacturing projects at LLNL. He is also the founder and leader of a new additive manufacturing and process development laboratory at LLNL. The work in this lab focuses on developing next generation additive processes which are capable of micro- and nano-scale features and have the ability to create components with mixtures of materials ranging from polymers to metals and ceramics. Development of these processes also involves the synthesis and materials science of feedstocks such as photopolymers and nanoparticles. These capabilities are utilized to fabricate microarchitected materials with unique designer properties such as negative thermal expansion or ultra-light weight materials with a high stiffness.

Spadaccini has been a member of the technical staff in the Materials Engineering Division and the Center for Micro and Nano Technology at LLNL for the past nine years. He received the S.B., S.M., and Ph.D. degrees from the Department of Aeronautics and Astronautics at the Massachusetts Institute of Technology (MIT) in 1997, 1999, and 2004, respectively. He has authored over three dozen journal and conference publications, two book chapters, has multiple patents awarded, and has several patents under review. Dr. Spadaccini is also a part-time faculty member at the San Jose State University in the Biomedical, Chemical and Materials Engineering Department, where he teaches graduate courses in advanced transport phenomena.

Additive Manufacturing: State of the Industry

U.S. Department of State
February 24, 2014

Tim Caffrey

WOHLERS
ASSOCIATES

Growth trends

Export controls and 3D-printed guns

Myths and misconceptions

Developments around the world

Glimpse of the future

WOHLERS
ASSOCIATES



Additive



Overview of Additive Technologies



Subtractive

Formative



Copyright 2012

Terminology

additive manufacturing

3D printing

formal standard

de facto standard

technical media

mainstream media

scientific community

everyone else

Google: 10M

Google: 286M

Terms are used interchangeably

WOHLERS
ASSOCIATES



**ASTM International
Committee F42 on Additive
Manufacturing Technologies**

Boeing, DePuy Spine, GE, Goodrich, Honeywell, Lockheed
Martin, NIST, Raytheon, Siemens, U.S. Army

material extrusion

directed energy deposition

material jetting

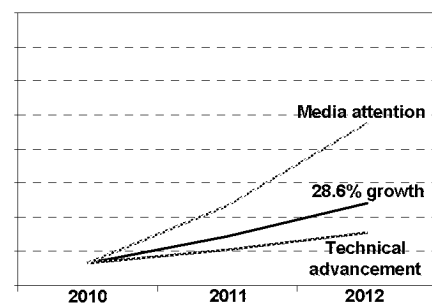
vat photopolymerization

binder jetting

sheet lamination

powder bed fusion

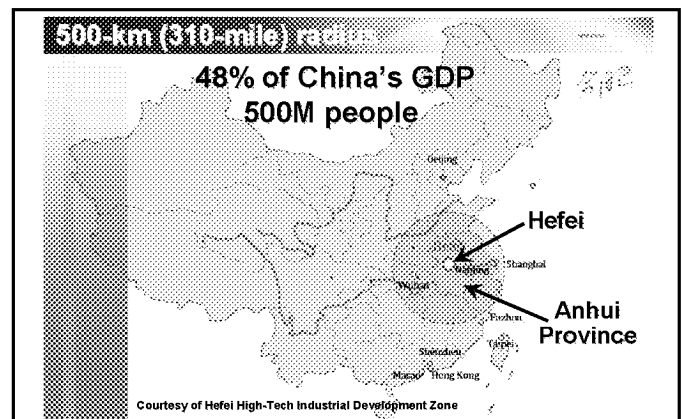
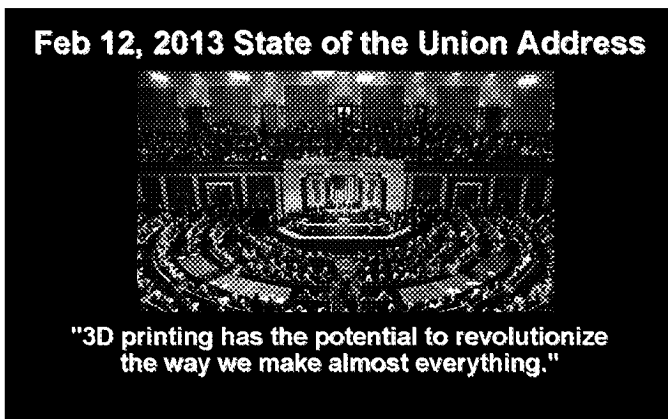
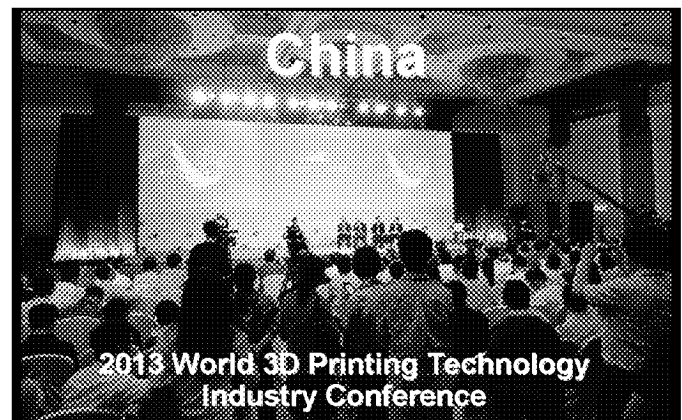
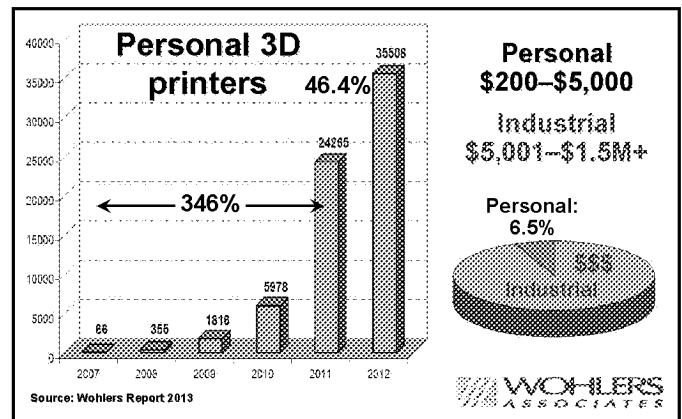
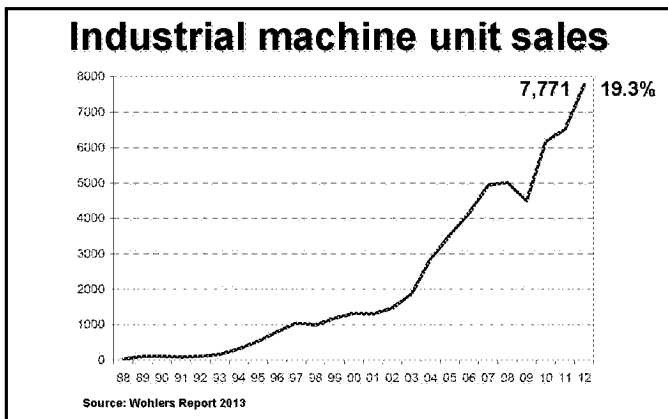
WOHLERS
ASSOCIATES



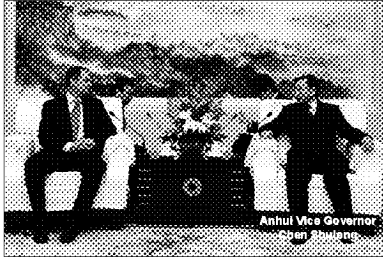
Source: Wohlers Associates, Inc.

Investment
New products
Startups
Events
Governments
Research
Personal use
Awareness
Kickstarter

WOHLERS
ASSOCIATES



Anhui Province: 67 million people



"3D printing will become very important to China and Anhui Province."

Investing 750M yuan (\$120M)
in AM over next 3 years

Another \$120M over the
following 3 years

One strategy: buy its way in

Singapore

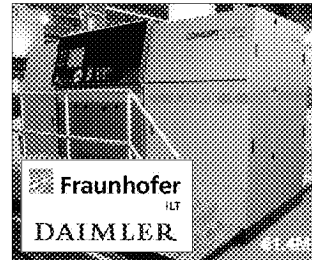
Building a 3D printing ecosystem

\$S500M (US\$400M) in a 5-year
advanced manufacturing program

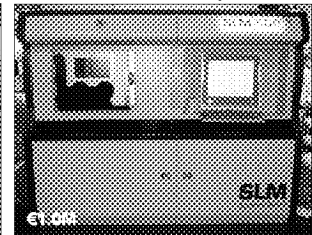
Germany

630 x 400 x 500 (24.8 x 15.7 x 19.7)
1 kW variable focus laser

500 x 280 x 325 (19.7 x 11 x 12.8)
2.8 kW of total laser power



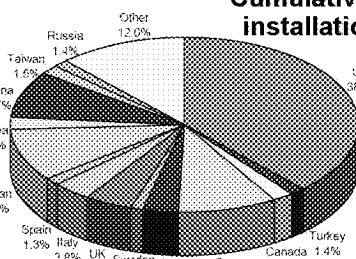
Courtesy of Concept Laser



Courtesy of SLM Solutions

United States

Cumulative industrial AM
installations worldwide

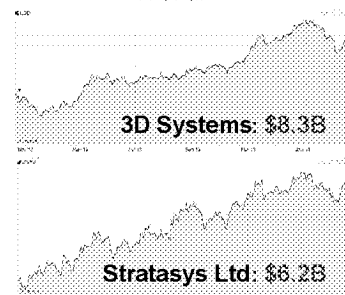


Most history,
users, experience,
and know-how

Source: Wohlers Report 2013

WOHLERS
ASSOCIATES


U.S. has 2 largest companies had



Source: Yahoo! Finance

Registered
in Israel

WOHLERS
ASSOCIATES

 **GE Aviation**

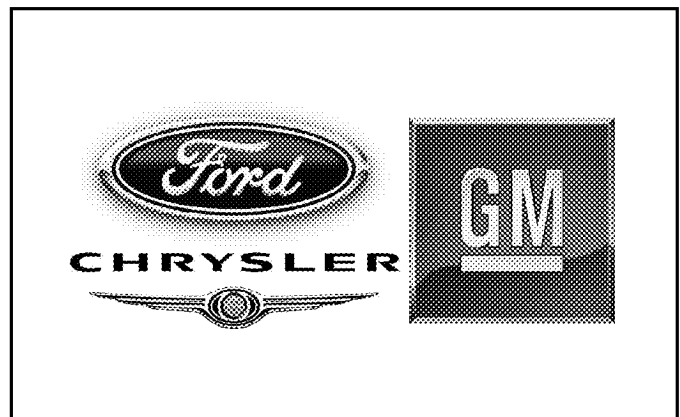
\$3.5B in 5 years

New design: 32,300 per year

25% lighter, 5x more durable

Old design

Images courtesy of GE Aviation



National Additive Manufacturing Innovation Institute

 **America Makes**

When America Makes America Works

Funding

Fiscal Year	FY12	FY13	FY14	Total
Approx. Date of Fund Allocation	15 Aug 2012 (upon award)	1 Mar 2013	1 Mar 2014	
Amount	\$18.8M	\$4.0M	\$7.2M	\$30.0M

Funding provided from multiple government agencies: OSD, Army, DARPA, DOE, NSF, NASA

At minimum, a 50/50 cost share

Industrial AM system manufacturers

16 in Europe

7 in China

5 in U.S. (4 sold 35 systems in 2012)



Lost some of its edge in AM

Thousands of new companies and businesses

U.S. is a nation of business-minded innovators and independent thinkers

Easy to start a new company



Export controls

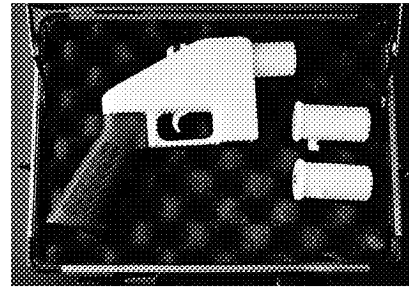
No benefit to U.S. manufacturing
or national security

No positive effect on
global competitiveness in AM

Would likely hurt U.S.
AM system manufacturers

WOHLERS
ASSOCIATES

3D-printed guns



Courtesy of Cody Wilson

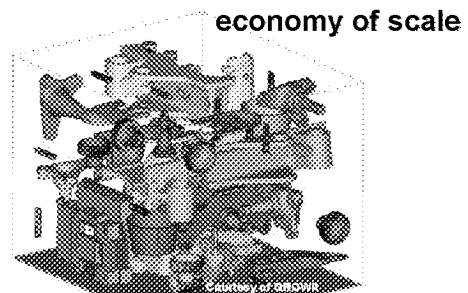
WOHLERS
ASSOCIATES

Myths and misconceptions

Push button
data preparation
file repair
setting of build parameters
preheating
build
cooling
support removal
finishing

WOHLERS
ASSOCIATES

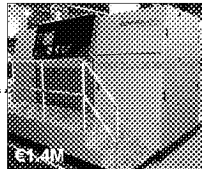
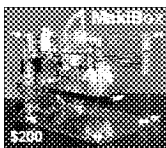
Just as inexpensive to build one part at a time



economy of scale

Courtesy of BROWN

Systems and materials are inexpensive



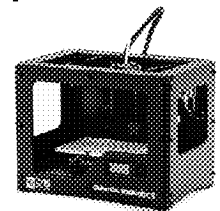
Plastic materials: 53–104x more expensive

WOHLERS
ASSOCIATES

Everyone will own and operate a general-purpose 3D printer

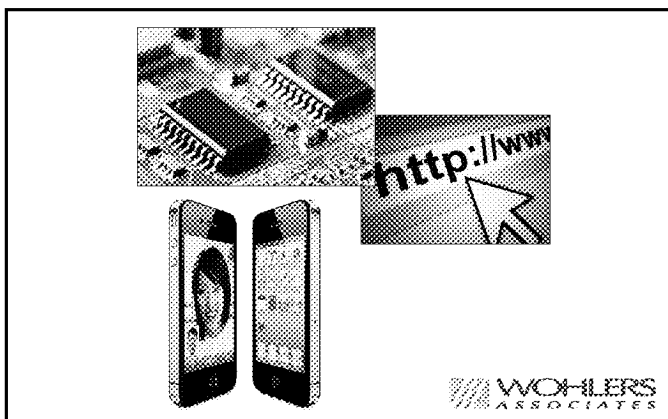
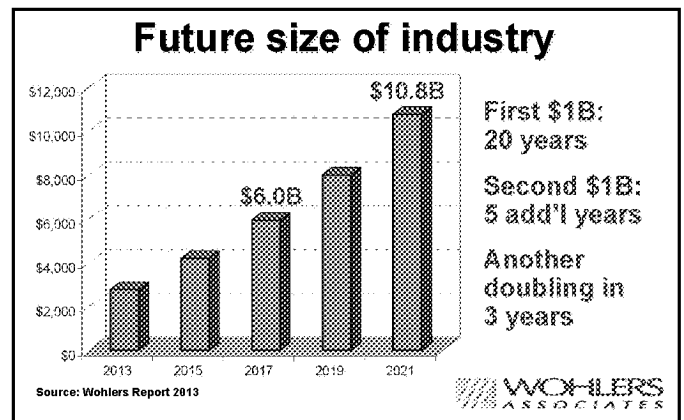
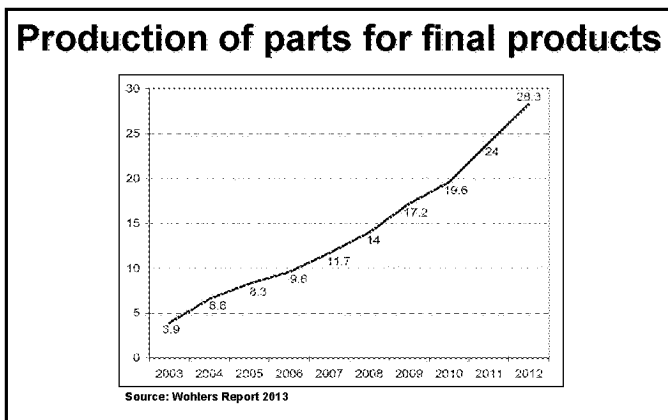
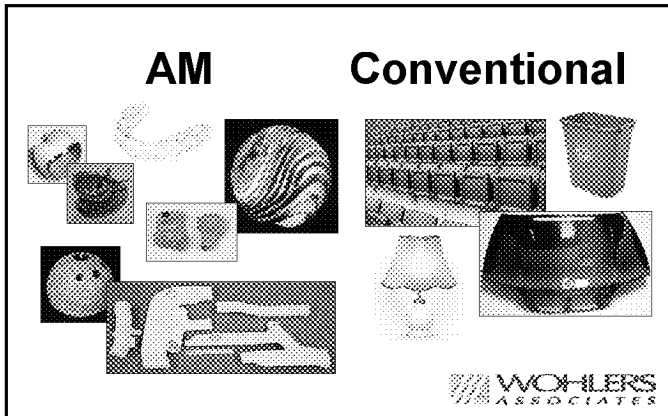


write
present
communicate
calculate
listen to music
organize pictures
maintain records
research



Source: Ian Campbell, Loughborough University

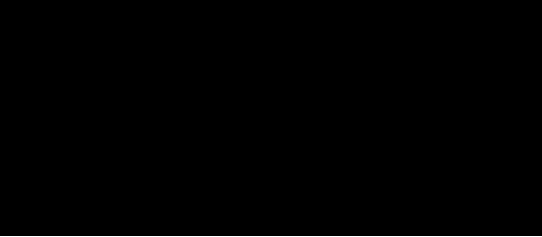
WOHLERS
ASSOCIATES



NO DISCERNIBLE CLASSIFICATION

From: [REDACTED]
Sent: Wednesday, April 15, 2015 2:39 PM
To: [REDACTED]
Subject: Forget 3D printed guns, how about 3D printed SLVs

<http://www.engadget.com/2015/04/15/rocket-lab-rutherford-engine>



This email is UNCLASSIFIED.

NO DISCERNIBLE CLASSIFICATION

Startup launches first 3D-printed battery-powered rocket (update)



Maricelis Moon
Be 15.16 in Space

Rocket Lab is a Lockheed Martin-funded startup that dreams of taking small satellites to space for an affordable price -- but it wants to do so using technology quite different than usual. See, the company has revealed that its engine called the "Rutherford" is (1) composed mostly of 3D-printed parts, and (2) uses batteries ~~instead of liquid fuel~~. It will be paired up with the company's Electron launch system, and together they make up the first battery-powered rocket, or so the startup claims. Its batteries power the turbopumps that deliver propellant to the engine.*

The company says it takes merely three days to print the components of the Rutherford engine out of titanium and other alloys, using an advanced form of 3D printing called "electron beam melting." (If those components are manufactured via traditional means, it will take up to a month instead.) That means Rocket Labs', well, rockets can be manufactured faster and will cost clients less money per launch. In fact, the startup believes it will cost only around \$4.9 million to send the 65 feet x 3 feet system to space, carrying a payload that weighs up to 220 pounds. It plans to start ferrying satellites and other payloads out there in 2016.

Update: As many of you pointed out, the Rutherford-Electron rocket doesn't use electric propulsion and still uses liquid fuel like typical rockets. We apologize for the confusion. [Thanks, Nik and RiotingSpectre]

Via: Popular Science

DOSWASHINGTON000035

Source: Rocket Lab, Reuters

in this

article: 3dPrinting, battery, design, electricrocket, electronrocket,gadgetry, gadgets, rocket, rutherfordengine, satellite, space,timeline1

hearing,” which are conducted pursuant to the provisions of 5 U.S.C. 556 and 557. The CSA sets forth the criteria for scheduling a drug or other substance and for removing a drug or substance from the schedules of controlled substances. Such actions are exempt from review by the Office of Management and Budget (OMB) pursuant to section 3(d)(1) of Executive Order 12866 and the principles reaffirmed in Executive Order 13563.

Executive Order 12988

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 Civil Justice Reform to eliminate drafting errors and ambiguity, minimize litigation, provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

Executive Order 13132

This rulemaking does not have federalism implications warranting the application of Executive Order 13132. The rule does not have substantial direct effects on the States, on the relationship between the Federal Government and the States, or the distribution of power and responsibilities among the various levels of government.

Executive Order 13175

This rule does not have tribal implications warranting the application of Executive Order 13175. This rule does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

Regulatory Flexibility Act

The Administrator, in accordance with the Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA), has reviewed this proposed rule and by approving it certifies that it will not have a significant economic impact on a substantial number of small entities. The purpose of this rule is to remove [¹²³I]ioflupane from the list of schedules of the CSA. This action will remove regulatory controls and administrative, civil, and criminal sanctions applicable to controlled substances for handlers and proposed handlers of [¹²³I]ioflupane. Accordingly, it has the potential for some economic impact in the form of cost savings.

If finalized, the proposed rule will affect all persons who would handle, or propose to handle, [¹²³I]ioflupane. Due to the wide variety of unidentifiable and

unquantifiable variables that potentially could influence the distribution and administration rates of new molecular entities, the DEA is unable to determine the number of entities and small entities which might handle [¹²³I]ioflupane.

Although the DEA does not have a reliable basis to estimate the number of affected entities and quantify the economic impact of this proposed rule, a qualitative analysis indicates that, if finalized, this rule is likely to result in some cost savings for the healthcare industry. The affected entities will continue to meet existing Federal and/or state requirements applicable to those who handle radiopharmaceutical substances, including licensure, security, recordkeeping, and reporting requirements, which in many cases are more stringent than the DEA’s requirements. However, the DEA estimates cost savings will be realized from the removal of the administrative, civil, and criminal sanctions for those entities handling or proposing to handle [¹²³I]ioflupane, in the form of saved registration fees, and the elimination of additional physical security, recordkeeping, and reporting requirements.

Because of these facts, this rule will not result in a significant economic impact on a substantial number of small entities.

Unfunded Mandates Reform Act of 1995

On the basis of information contained in the “Regulatory Flexibility Act” section above, the DEA has determined and certifies pursuant to the Unfunded Mandates Reform Act of 1995 (UMRA), 2 U.S.C. 1501 *et seq.*, that this action would not result in any federal mandate that may result “in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100,000,000 or more (adjusted for inflation) in any one year * * *.” Therefore, neither a Small Government Agency Plan nor any other action is required under provisions of UMRA.

Paperwork Reduction Act

This action does not impose a new collection of information requirement under the Paperwork Reduction Act, 44 U.S.C. 3501–3521. This action would not impose recordkeeping or reporting requirements on State or local governments, individuals, businesses, or organizations. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

List of Subjects in 21 CFR part 1308

Administrative practice and procedure, Drug traffic control, Reporting and recordkeeping requirements.

For the reasons set out above, 21 CFR part 1308 is proposed to be amended to read as follows:

PART 1308—SCHEDULES OF CONTROLLED SUBSTANCES

■ 1. The authority citation for 21 CFR part 1308 continues to read as follows:

Authority: 21 U.S.C. 811, 812, 871(b), unless otherwise noted.

■ 2. In § 1308.12, revise paragraph (b)(4) to read as follows:

§ 1308.12 Schedule II.

* * * * *

(b) * * *

(4) Coca leaves (9040) and any salt, compound, derivative or preparation of coca leaves (including cocaine (9041) and ecgonine (9180) and their salts, isomers, derivatives and salts of isomers and derivatives), and any salt, compound, derivative, or preparation thereof which is chemically equivalent or identical with any of these substances, except that the substances shall not include:

- (i) Decocainized coca leaves or extraction of coca leaves, which extractions do not contain cocaine or ecgonine; or
- (ii) [¹²³I]ioflupane.

* * * * *

Dated: May 6, 2015.

Michele M. Leonhart,
Administrator.

[FR Doc. 2015–13455 Filed 6–2–15; 8:45 am]

BILLING CODE 4410–09–P

DEPARTMENT OF STATE

22 CFR Parts 120, 123, 125, and 127

[Public Notice 9149]

RIN 1400–AD70

International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

AGENCY: Department of State.

ACTION: Proposed rule.

SUMMARY: As part of the President’s Export Control Reform (ECR) initiative, the Department of State proposes to amend the International Traffic in Arms

Regulations (ITAR) to update the definitions of “defense article,” “defense services,” “technical data,” “public domain,” “export,” and “reexport or retransfer” in order to clarify the scope of activities and information that are covered within these definitions and harmonize the definitions with the Export Administration Regulations (EAR), to the extent appropriate. Additionally, the Department proposes to create definitions of “required,” “technical data that arises during, or results from, fundamental research,” “release,” “retransfer,” and “activities that are not exports, reexports, or retransfers” in order to clarify and support the interpretation of the revised definitions that are proposed in this rulemaking. The Department proposes to create new sections detailing the scope of licenses, unauthorized releases of information, and the “release” of secured information, and revises the sections on “exports” of “technical data” to U.S. persons abroad. Finally, the Department proposes to address the electronic transmission and storage of unclassified “technical data” via foreign communications infrastructure. This rulemaking proposes that the electronic transmission of unclassified “technical data” abroad is not an “export,” provided that the data is sufficiently secured to prevent access by foreign persons. Additionally, this proposed rule would allow for the electronic storage of unclassified “technical data” abroad, provided that the data is secured to prevent access by parties unauthorized to access such data. The revisions contained in this proposed rule are part of the Department of State’s retrospective plan under Executive Order 13563 first submitted on August 17, 2011.

DATES: The Department of State will accept comments on this proposed rule until August 3, 2015.

ADDRESSES: Interested parties may submit comments within 60 days of the date of publication by one of the following methods:

- *Email:* DDTCTPublicComments@state.gov with the subject line, “ITAR Amendment—Revisions to Definitions; Data Transmission and Storage.”
- *Internet:* At www.regulations.gov, search for this notice by using this rule’s RIN (1400–AD70).

Comments received after that date may be considered, but consideration cannot be assured. Those submitting comments should not include any personally identifying information they do not desire to be made public or information for which a claim of

confidentiality is asserted because those comments and/or transmittal emails will be made available for public inspection and copying after the close of the comment period via the Directorate of Defense Trade Controls Web site at www.pmdtdc.state.gov. Parties who wish to comment anonymously may do so by submitting their comments via www.regulations.gov, leaving the fields that would identify the commenter blank and including no identifying information in the comment itself. Comments submitted via www.regulations.gov are immediately available for public inspection.

FOR FURTHER INFORMATION CONTACT: Mr. C. Edward Peartree, Director, Office of Defense Trade Controls Policy, Department of State, telephone (202) 663–1282; email DDTCResponseTeam@state.gov. ATTN: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage. The Department of State’s full retrospective plan can be accessed at <http://www.state.gov/documents/organization/181028.pdf>.

SUPPLEMENTARY INFORMATION: The Directorate of Defense Trade Controls (DDTC), U.S. Department of State, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130). The items subject to the jurisdiction of the ITAR, *i.e.*, “defense articles” and “defense services,” are identified on the ITAR’s U.S. Munitions List (USML) (22 CFR 121.1). With few exceptions, items not subject to the export control jurisdiction of the ITAR are subject to the jurisdiction of the Export Administration Regulations (“EAR,” 15 CFR parts 730 through 774, which includes the Commerce Control List (CCL) in Supplement No. 1 to part 774), administered by the Bureau of Industry and Security (BIS), U.S. Department of Commerce. Both the ITAR and the EAR impose license requirements on exports and reexports. Items not subject to the ITAR or to the exclusive licensing jurisdiction of any other set of regulations are subject to the EAR.

BIS is concurrently publishing comparable proposed amendments (BIS companion rule) to the definitions of “technology,” “required,” “peculiarly responsible,” “published,” results of “fundamental research,” “export,” “reexport,” “release,” and “transfer (in-country)” in the EAR. A side-by-side comparison on the regulatory text proposed by both Departments is available on both agencies’ Web sites: www.pmdtdc.state.gov and www.bis.doc.gov.

1. Revised Definition of Defense Article

The Department proposes to revise the definition of “defense article” to clarify the scope of the definition. The current text of § 120.6 is made into a new paragraph (a), into which software is added to the list of things that are a “defense article” because software is being removed from the definition of “technical data.” This is not a substantive change.

A new § 120.6(b) is added to list those items that the Department has determined should not be a “defense article,” even though they would otherwise meet the definition of “defense article.” All the items described were formerly excluded from the definition of “technical data” in § 120.10. These items are declared to be not subject to the ITAR to parallel the EAR concept of “not subject to the EAR” as part of the effort to harmonize the ITAR and the EAR. This does not constitute a change in policy regarding these items or the scope of items that are defense articles.

2. Revised Definition of Technical Data

The Department proposes to revise the definition of “technical data” in ITAR § 120.10 in order to update and clarify the scope of information that may be captured within the definition. Paragraph (a)(1) of the revised definition defines “technical data” as information “required” for the “development,” “production,” operation, installation, maintenance, repair, overhaul, or refurbishing of a “defense article,” which harmonizes with the definition of “technology” in the EAR and the Wassenaar Arrangement. This is not a change in the scope of the definition, and additional words describing activities that were in the prior definition are included in parentheses to assist exporters.

Paragraph (a)(1) also sets forth a broader range of examples of formats that “technical data” may take, such as diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, or electronic media, that may constitute “technical data.” Additionally, the revised definition includes certain conforming changes intended to reflect the revised and newly added defined terms proposed elsewhere in this rule.

The proposed revised definition also includes a note clarifying that the modification of the design of an existing item creates a new item and that the “technical data” for the modification is “technical data” for the new item.

Paragraph (a)(2) of the revised definition defines “technical data” as

also including information that is enumerated on the USML. This will be “technical data” that is positively described, as opposed to “technical data” described in the standard catch-all “technical data” control for all “technical data” directly related to a “defense article” described in the relevant category. The Department intends to enumerate certain controlled “technical data” as it continues to move the USML toward a more positive control list.

Paragraph (a)(3) of the revised definition defines “technical data” as also including classified information that is for the “development,” “production,” operation, installation, maintenance, repair, overhaul, or refurbishing of a “defense article” or a 600 series item subject to the EAR. Paragraph (a)(5) of the revised definition defines “technical data” as also including information to access secured “technical data” in clear text, such as decryption keys, passwords, or network access codes. In support of the latter change, the Department also proposes to add a new provision to the list of violations in § 127.1(b)(4) to state that any disclosure of these decryption keys or passwords that results in the unauthorized disclosure of the “technical data” or software secured by the encryption key or password is a violation and will constitute a violation to the same extent as the “export” of the secured information. For example, the “release” of a decryption key may result in the unauthorized disclosure of multiple files containing “technical data” hosted abroad and could therefore constitute a violation of the ITAR for each piece of “technical data” on that server.

Paragraph (b) of the revised definition of “technical data” excludes non-proprietary general system descriptions, information on basic function or purpose of an item, and telemetry data as defined in Note 3 to USML Category XV(f) (§ 121.1). Items formerly identified in this paragraph, principles taught in schools and “public domain” information, have been moved to the new ITAR § 120.6(b).

The proposed definition removes software from the definition of “technical data.” Specific and catch-all controls on software will be added elsewhere throughout the ITAR as warranted, as it will now be defined as a separate type of “defense article.”

3. Proposed Definition of Required

The Department proposes a definition of “required” in a new § 120.46. “Required” is used in the definition of “technical data” and has, to this point,

been an undefined term in the ITAR. The word is also used in the controls on technology in both the EAR and the Wassenaar Arrangement, as a defined term, which the Department is now proposing to adopt:

. . . [O]nly that portion of [technical data] that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required [technical data] may be shared by different products.

The proposed definition of “required” contains three notes. These notes explain how the definition is to be applied.

Note 1 provides that the definition explicitly includes information for meeting not only controlled performance levels, but also characteristics and functions. All items described on the USML are identified by a characteristic or function. Additionally, some descriptions include a performance level. As an example, USML Category VIII(a)(1) controls aircraft that are “bombers” and contains no performance level. The characteristic of the aircraft that is controlled is that it is a bomber, and therefore, any “technical data” peculiar to making an aircraft a bomber is “required.”

Note 2 states that, with the exception of “technical data” specifically enumerated on the USML, the jurisdictional status of unclassified “technical data” is the same as that of the commodity to which it is directly related. Specifically, it explains that “technical data” for a part or component of a “defense article” is directly related to that part or component, and if the part or component is subject to the EAR, so is the “technical data.”

Note 3 establishes a test for determining if information is peculiarly responsible for meeting or achieving the controlled performance levels, characteristics or functions of a “defense article.” It uses the same catch-and-release concept that the Department implemented in the definition of “specially designed.” It has a similarly broad catch of all information used in or for use in the “development,” “production,” operation, installation, maintenance, repair, overhaul, or refurbishing of a “defense article.” It has four releases that mirror the “specially designed” releases, and one reserved paragraph for information that the Department determines is generally insignificant. The first release is for information identified in a commodity jurisdiction determination. The second release is reserved. The third release is for information that is identical to information used in a non-defense

article that is in “production,” and not otherwise enumerated on the ITAR. The fourth release is for information that was developed with knowledge that it is for both a “defense article” and a non-defense article. The fifth release is information that was developed for general purpose commodities.

In the companion rule, BIS proposes to make Note 3 into a stand-alone definition for “peculiarly responsible” as it has application outside of the definition of “required.” The substance of Note 3 and the BIS definition of “peculiarly responsible” are identical. DDTC asks for comments on the placement of this concept.

4. Proposed Definitions of Development and Production

The Department proposes to add § 120.47 for the definition of “development” and § 120.48 for the definition of “production.” These definitions are currently in Notes 1 and 2 to paragraph (b)(3) in § 120.41, the definition of “specially designed.” Because “technical data” is now defined, in part, as information “required” for the “development” or “production” of a “defense article,” and these words are now used in the definition of a “defense service,” it is appropriate to define these terms. The adoption of these definitions is also done for the purpose of harmonization because these definitions are also used in the EAR and by the Wassenaar Arrangement.

5. Revised Definition of Public Domain

The Department proposes to revise the definition of “public domain” in ITAR § 120.11 in order to simplify, update, and introduce greater versatility into the definition. The existing version of ITAR § 120.11 relies on an enumerated list of circumstances through which “public domain” information might be published. The Department believes that this definition is unnecessarily limiting in scope and insufficiently flexible with respect to the continually evolving array of media, whether physical or electronic, through which information may be disseminated.

The proposed definition is intended to identify the characteristics that are common to all of the enumerated forms of publication identified in the current rule—with the exception of ITAR § 120.11(a)(8), which is addressed in a new definition for “technical data that arises during, or results from, fundamental research”—and to present those common characteristics in a streamlined definition that does not require enumerated identification

within the ITAR of every current or future qualifying publication scenario. Additionally, the proposed definition incorporates phrases such as “generally accessible” and “without restriction upon its further dissemination” in order to better align the definition found in the EAR and more closely aligned with the definition in the Wassenaar Arrangement control lists.

The proposed definition requires that information be made available to the public without restrictions on its further dissemination. Any information that meets this definition is “public domain.” The definition also retains an exemplary list of information that has been made available to the public without restriction and would be considered “public domain.” These include magazines, periodicals and other publications available as subscriptions, publications contained in libraries, information made available at a public conference, meeting, seminar, trade show, or exhibition, and information posted on public Web sites. The final example deems information that is submitted to co-authors, editors, or reviewers or conference organizers for review for publication to be “public domain,” even prior to actual publication. The relevant restrictions do not include copyright protections or generic property rights in the underlying physical medium.

Paragraph (b) of the revised definition explicitly sets forth the Department’s requirement of authorization to release information into the “public domain.” Prior to making available “technical data” or software subject to the ITAR, the U.S. government must approve the release through one of the following: (1) The Department; (2) the Department of Defense’s Office of Security Review; (3) a relevant U.S. government contracting authority with authority to allow the “technical data” or software to be made available to the public, if one exists; or (4) another U.S. government official with authority to allow the “technical data” or software to be made available to the public.

The requirements of paragraph (b) are not new. Rather, they are a more explicit statement of the ITAR’s requirement that one must seek and receive a license or other authorization from the Department or other cognizant U.S. government authority to release ITAR controlled “technical data,” as defined in § 120.10. A release of “technical data” may occur by disseminating “technical data” at a public conference or trade show, publishing “technical data” in a book or journal article, or posting “technical data” to the Internet. This proposed provision will enhance

compliance with the ITAR by clarifying that “technical data” may not be made available to the public without authorization. Persons who intend to discuss “technical data” at a conference or trade show, or to publish it, must ensure that they obtain the appropriate authorization.

Information that is excluded from the definition of “defense article” in the new § 120.6(b) is not “technical data” and therefore does not require authorization prior to release into the “public domain.” This includes information that arises during or results from “fundamental research,” as described in the new § 120.49; general scientific, mathematical, or engineering principles commonly taught in schools, and information that is contained in patents.

The Department also proposes to add a new provision to § 127.1 in paragraph (a)(6) to state explicitly that the further dissemination of “technical data” or software that was made available to the public without authorization is a violation of the ITAR, if, and only if, it is done with knowledge that the “technical data” or software was made publicly available without an authorization described in ITAR § 120.11(b)(2). Dissemination of publicly available “technical data” or software is not an export-controlled event, and does not require authorization from the Department, in the absence of knowledge that it was made publicly available without authorization.

“Technical data” and software that is made publicly available without proper authorization remains “technical data” or software and therefore remains subject to the ITAR. As such, the U.S. government may advise a person that the original release of the “technical data” or software was unauthorized and put that person on notice that further dissemination would violate the ITAR.

6. Proposed Definition of Technical Data That Arises During, or Results From, Fundamental Research

The Department proposes to move “fundamental research” from the definition of “public domain” in ITAR § 120.11(a)(8) and define “technical data that arises during, or results from, fundamental research” in a new ITAR § 120.49. The Department believes that information that arises during, or results from fundamental research is conceptually distinguishable from the information that would be captured in the revised definition of “public domain” that is proposed in this rule. Accordingly, the Department proposes to address this concept with its own definition. The new definition of

“technical data that arises during, or results from, fundamental research” is consistent with the prior ITAR § 120.11(a)(8), except that the Department has expanded the scope of eligible research to include research that is funded, in whole or in part, by the U.S. government.

7. Revised Definition of Export

The Department proposes to revise the definition of “export” in ITAR § 120.17 to better align with the EAR’s revised definition of the term and to remove activities associated with a defense article’s further movement or release outside the United States, which will now fall within the definition of “reexport” in § 120.19. The definition is revised to explicitly identify that ITAR §§ 126.16 and 126.17 (exemptions pursuant to the Australia and UK Defense Trade Cooperation Treaties) have their own definitions of “export,” which apply exclusively to those exemptions. It also explicitly references the new § 120.49, “Activities that are Not Exports, Reexports, or Retransfers,” which excludes from ITAR control certain transactions identified therein.

Paragraph (a)(1) is revised to parallel the definition of “export” in proposed paragraph (a)(1) of § 734.13 of the EAR. Although the wording has changed, the scope of the control is the same. The provision excepting travel outside of the United States by persons whose personal knowledge includes “technical data” is removed, but the central concept is unchanged. The “release” of “technical data” to a foreign person while in the United States or while travelling remains a controlled event.

Paragraph (a)(2) includes the control listed in the current § 120.17(a)(4) (transfer of technical data to a foreign person). The proposed revisions replace the word “disclosing” with “releasing,” and the paragraph is otherwise revised to parallel proposed paragraph (a)(2) of § 734.13 of the EAR. “Release” is a newly defined concept in § 120.50 that encompasses the previously undefined term “disclose.”

Paragraph (a)(3) includes the control listed in the current § 120.17(a)(2) (transfer of registration, control, or ownership to a foreign person of an aircraft, vessel, or satellite). It is revised to parallel proposed paragraph (a)(3) of § 734.13 of the EAR.

Paragraph (a)(4) includes the control listed in the current § 120.17(a)(3) (transfer in the United States to foreign embassies).

Paragraph (a)(5) maintains the control on performing a “defense service.”

Paragraph (a)(6) is added for the “release” or transfer of decryption keys,

passwords, and other items identified in the new paragraph (a)(5) of the revised definition of “technical data” in § 120.10. This paragraph makes “release” or transfer of information securing “technical data” an “export.” Making the release of decryption keys and other information securing technical data in an inaccessible or unreadable format an export allows the Department to propose that providing someone with encrypted “technical data” would not be an “export,” under certain circumstances. Provision of a decryption key or other information securing “technical data” is an “export” regardless of whether the foreign person has already obtained access to the secured “technical data.” Paragraph (a)(6) of the definitions of export and reexport in this rule and the BIS companion rule present different formulations for this control and the agencies request input from the public on which language more clearly describes the control. The agencies intend, however, that the act of providing physical access to unsecured “technical data” (subject to the ITAR) will be a controlled event. The mere act of providing access to unsecured technology (subject to the EAR) will not, however, be a controlled event unless it is done with “knowledge” that such provision will cause or permit the transfer of controlled “technology” in clear text or “software” to a foreign national.

Paragraph (a)(7) is added for the release of information to a public network, such as the Internet. This makes more explicit the existing control in (a)(4), which includes the publication of “technical data” to the Internet due to its inherent accessibility by foreign persons. This means that before posting information to the Internet, you should determine whether the information is “technical data.” You should review the USML, and if there is doubt about whether the information is “technical data,” you may request a commodity jurisdiction determination from the Department. If so, a license or other authorization, as described in § 120.11(b), will generally be required to post such “technical data” to the Internet. Posting “technical data” to the Internet without a Department or other authorization is a violation of the ITAR even absent specific knowledge that a foreign national will read the “technical data.”

Paragraph (b)(1) is added to clarify existing ITAR controls to explicitly state that disclosing “technical data” to a foreign person is deemed to be an “export” to all countries in which the

foreign person has held citizenship or holds permanent residency.

8. Revised Definition of Reexport

The Department proposes to revise the definition of “reexport” in ITAR § 120.19 to better align with the EAR’s revised definition and describe transfers of items subject to the jurisdiction of the ITAR between two foreign countries. The activities identified are the same as those in paragraphs (a)(1) through (4) of the revised definition of “export,” except that the shipment, release or transfer is between two foreign countries or is to a third country national foreign person outside of the United States.

9. Proposed Definition of Release

The Department proposes to add § 120.50, the definition of “release.” This term is added to harmonize with the EAR, which has long used the term to cover activities that disclose information to foreign persons. “Release” includes the activities encompassed within the undefined term “disclose.” The activities that are captured include allowing a foreign person to inspect a “defense article” in a way that reveals “technical data” to the foreign persons and oral or written exchanges of “technical data” with a foreign person. The adoption of the definition of “release” does not change the scope of activities that constitute an “export” and other controlled transactions under the ITAR.

10. Proposed Definition of Retransfer

The Department proposes to add § 120.51, the definition of “retransfer.” “Retransfer” is moved out of the definition of “reexport” in § 120.19 to better harmonize with the EAR, which controls “exports,” “reexports” and “transfers (in country)” as discrete events. Under this new definition, a “retransfer” occurs with a change of end use or end user within the same foreign territory. Certain activities may fit within the definition of “reexport” and “retransfer,” such as the disclosure of “technical data” to a third country national abroad. Requests for both “reexports” and “retransfers” of “defense articles” will generally be processed through a General Correspondence or an exemption.

11. Proposed Activities That Are Not Exports, Reexports, or Retransfers

The Department proposes to add § 120.52 to describe those “activities that are not exports, reexports, or retransfers” and do not require authorization from the Department. It is not an “export” to launch items into

space, provide “technical data” or software to U.S. persons while in the United States, or move a “defense article” between the states, possessions, and territories of the United States. The Department also proposes to add a new provision excluding from ITAR licensing requirements the transmission and storage of encrypted “technical data” and software.

The Department recognizes that ITAR-controlled “technical data” may be electronically routed through foreign servers unbeknownst to the original sender. This presents a risk of unauthorized access and creates a potential for inadvertent ITAR violations. For example, email containing “technical data” may, without the knowledge of the sender, transit a foreign country’s Internet service infrastructure en route to its intended and authorized final destination. Any access to this data by a foreign person would constitute an unauthorized “export” under ITAR § 120.17. Another example is the use of mass data storage (*i.e.*, “cloud storage”). In this case, “technical data” intended to be resident in cloud storage may, without the knowledge of the sender, be physically stored on a server or servers located in a foreign country or multiple countries. Any access to this data, even if unintended by the sender, would constitute an “export” under ITAR § 120.17.

The intent of the proposed ITAR § 120.52(a)(4) is to clarify that when unclassified “technical data” transits through a foreign country’s Internet service infrastructure, a license or other approval is not mandated when such “technical data” is encrypted prior to leaving the sender’s facilities and remains encrypted until received by the intended recipient or retrieved by the sender, as in the case of remote storage. The encryption must be accomplished in a manner that is certified by the U.S. National Institute for Standards and Technology (NIST) as compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2). Additionally, the Department proposes that the electronic storage abroad of “technical data” that has been similarly encrypted would not require an authorization, so long as it is not stored in a § 126.1 country or in the Russian Federation. This will allow for cloud storage of encrypted data in foreign countries, so long as the “technical data” remains continuously encrypted while outside of the United States.

12. Revised Exemption for the Export of Technical Data for U.S. Persons Abroad

The Department proposes to revise § 125.4(b)(9) to better harmonize controls on the “release” of controlled information to U.S. persons abroad and to update the provisions. The most significant update is that foreign persons authorized to receive “technical data” in the United States will be eligible to receive that same “technical data” abroad, when on temporary assignment on behalf of their employer. The proposed revisions clarify that a person going abroad may use this exemption to “export” “technical data” for their own use abroad. The proposed revisions also clarify that the “technical data” must be secured while abroad to prevent unauthorized “release.” It has been long-standing Department practice to hold U.S. persons responsible for the “release” of “technical data” in their possession while abroad. However, given the nature of “technical data” and the proposed exception from licensing for transmission of secured “technical data,” the Department has determined it is necessary to implement an affirmative obligation to secure data while abroad.

13. Proposed Scope of License

The Department proposes to add § 123.28 to clarify the scope of a license, in the absence of a proviso, and to state that authorizations are granted based on the information provided by the applicant. This means that while providing false information to the U.S. government as part of the application process for the “export,” “reexport,” or “retransfer” of a “defense article” is a violation of the ITAR, it also may void the license.

14. Revised Definition of Defense Service

Proposed revisions of the “defense service” definition were published on April 13, 2011, RIN 1400–AC80 (*see* “International Traffic in Arms Regulations: Defense Services,” 76 FR 20590) and May 24, 2013 (*see* 78 FR 31444, RIN 1400–AC80). In those rules, the Department explained its determination that the scope of the current definition is overly broad, capturing certain forms of assistance or services that no longer warrant ITAR control.

The Department reviewed comments on that first proposed definition and, when the recommended changes added to the clarity of the regulation, the Department accepted them. For the Department’s evaluation of those public comments and recommendations regarding the April 13, 2011, proposed

rule (the first revision), *see* 78 FR 31444, May 24, 2013. The Department’s evaluation of the written comments and recommendations in response to the May 24, 2013 proposed rule (the second revision) follows.

Parties commenting on the second revision expressed concern that the definition of “defense service” in paragraph (a)(1) was premised on the use of “other than public domain information.” The observation was made that with the intent of removing from the definition of a “defense service” the furnishing of assistance using “public domain” information, but not basing the assistance on the use of “technical data,” the Department was continuing to require the licensing of activities akin to those that were based on the use of “public domain” information. The Department has fully revised paragraph (a)(1) to remove the use of the “other than public domain information” or “technical data” from the determination of whether an activity is a “defense service.” Furthermore, the Department has added a new provision declaring that the activities described in paragraph (a)(1) are not a “defense service” if performed by a U.S. person or foreign person in the United States who does not have knowledge of U.S.-origin “technical data” directly related to the “defense article” that is the subject of the assistance or training or another “defense article” described in the same USML paragraph prior to performing the service. A note is added to clarify that a person will be deemed to have knowledge of U.S.-origin “technical data” if the person previously participated in the “development” of a “defense article” described in the same USML paragraph, or accessed (physically or electronically) that “technical data.” A note is also added to clarify that those U.S. persons abroad who only received U.S.-origin “technical data” as a result of their activities on behalf of a foreign person are not included within the scope of paragraph (a)(1). A third note is added to clarify that DDTC-authorized foreign person employees in the United States who provide “defense services” on behalf of their U.S. employer are considered to be included with the U.S. employer’s authorization, and need not be listed on the U.S. employer’s technical assistance agreement or receive a separate authorization for those services. The Department also removed the activities of design, development, and engineering from paragraph (a)(1) and moved them to paragraph (a)(2).

Commenting parties recommended revising paragraph (a)(1) to remove the

provision of “technical data” as a “defense service,” because there are already licensing requirements for the “export” of “technical data.” The Department confirms that it eliminated from the definition of a “defense service” the act of furnishing “technical data” to a foreign person. Such activity still constitutes an “export” and would require an ITAR authorization. New paragraph (a)(1) is concerned with the furnishing of assistance, whereas the “export” of “technical data” alone, without the furnishing of assistance, is not a “defense service.” The “export” of “technical data” requires an authorization (Department of State form DSP–5 or DSP–85) or the use of an applicable exemption.

Commenting parties recommended the definition be revised to explicitly state that it applies to the furnishing of assistance by U.S. persons, or by foreign persons in the United States. The Department partially accepted this recommendation. However, the Department notes that ITAR § 120.1(c) provides that only U.S. persons and foreign governmental entities in the United States may be granted a license or other approval pursuant to the ITAR, and that foreign persons may only receive a “reexport” or “retransfer” approval or approval for brokering activities. Therefore, approval for the performance of a defense service in the United States by a foreign person must be obtained by a U.S. person, such as an employer, on behalf of the foreign person. Regarding a related recommendation, the Department also notes that the furnishing of a type of assistance described by the definition of a “defense service” is not an activity within the Department’s jurisdiction when it is provided by a foreign person outside the United States to another foreign person outside the United States on a foreign “defense article” using foreign-origin “technical data.”

In response to commenting parties, the Department specified that the examples it provided for activities that are not “defense services” are not exhaustive. Rather, they are provided to answer the more frequent questions the Department receives on the matter. The Department removed these examples from paragraph (b) and included them as a note to paragraph (a).

A commenting party recommended that paragraphs (a)(5) and (a)(6), regarding the furnishing of assistance in the integration of a spacecraft to a launch vehicle and in the launch failure analysis of a spacecraft or launch vehicle, respectively, be removed, and that those activities be described in the USML categories covering spacecraft

and launch vehicles, on the basis that a general definition should not have such program-specific clauses. As discussed in the May 13, 2014 interim final rule revising USML Category XV (79 FR 27180), the Department accepted this recommendation and revised paragraph (f) of USML Category XV and paragraph (i) of USML Category IV accordingly. The revision includes the recommendation of commenting parties to specifically provide that the service must be provided to a foreign person in order for it to be a licensable activity.

Commenting parties recommended the Department define the term “tactical employment,” so as to clarify what services would be captured by paragraph (a)(3). The Department determined that employment of a “defense article” should remain a controlled event, due to the nature of items now controlled in the revised USML categories. After ECR, those items that remain “defense articles” are the most sensitive and militarily critical equipment that have a significant national security or intelligence application. Allowing training and other services to foreign nationals in the employment of these “defense articles” without a license would not be appropriate. Therefore, the Department removed the word “tactical” and converted the existing exemption for basic operation of a “defense article,” authorized by the U.S. government for “export” to the same recipient, into an exclusion from paragraph (a)(3).

A commenting party recommended the Department address the instance of the integration or installation of a “defense article” into an item, much as it addressed the instance of the integration or installation of an item into a “defense article.” Previously, the Department indicated this would be the subject of a separate rule, and addressed the “export” of such items in a proposed rule (*see* 76 FR 13928), but upon review the Department accepted this recommendation, and revised paragraph (a)(2), the note to paragraph (a)(2), and the note to paragraph (a) accordingly. In addition, the Department has changed certain terminology used in the paragraph: instead of referring to the “transfer” of “technical data,” the paragraph is premised on the “use” of “technical data.” This change is consistent with removing from the definition of a “defense service” the furnishing of “technical data” to a foreign person when there is not also the furnishing of assistance related to that “technical data.”

A commenting party requested clarification of the rationale behind

selectively excepting from the “defense services” definition the furnishing of services using “public domain” information. The Department did so in paragraph (a)(1), and now excludes those services performed by U.S. persons who have not previously had access to any U.S. origin “technical data” on the “defense article” being serviced. In contrast, the Department did not do so in paragraphs (a)(2) and (a)(3) and former paragraphs (a)(5) and (a)(6). In the case of paragraph (a)(2), the rationale for not doing so is that the activities involved in the development of a “defense article,” or in integrating a “defense article” with another item, inherently involve the advancement of the military capacity of another country and therefore constitute activities over which the U.S. government has significant national security and foreign policy concerns. To the extent that an activity listed in paragraph (a)(1), such as modification or testing, is done in the “development” of a “defense article,” such activities constitute “development” and are within the scope of paragraph (a)(2). With regard to paragraph (a)(3), the furnishing of assistance (including training) in the employment of a “defense article” is a type of activity that the Department believes warrants control as a “defense service,” due to the inherently military nature of providing training and other services in the employment of a “defense article” (changes to paragraph (a)(3) are described above). The services described in former paragraphs (a)(5) and (a)(6) (and now in USML Categories IV(i) and XV(f)) are pursuant to Public Law 105–261.

A commenting party recommended limiting paragraph (a)(2) to the integration of ECCN 9A515 and 600 series items into defense articles, saying that the regulations should focus on items subject to the EAR with a military or space focus. The Department’s focus with this provision is in fact the “defense article.” Items that are to be integrated with a “defense article,” which may not themselves be defense articles, may be beyond the authority of the Department to regulate. The Department did not accept this recommendation.

A commenting party recommended limiting the definition of integration to changes in the function of the “defense article,” and to exclude modifications in fit. For the purposes of illustration, this commenting party used one of the examples provided by the Department in the note to paragraph (a)(2): The manufacturer of the military vehicle will need to know the dimensions and electrical requirements of the dashboard

radio when designing the vehicle. In this instance, paragraph (a)(2) would not apply, as this example addresses the manufacture of a “defense article,” which is covered by paragraph (a)(1). If the radio to be installed in this vehicle is subject to the EAR, the provision to the manufacturer of information regarding the radio is not within the Department’s licensing jurisdiction. In an instance of a service entailing the integration of an item with a “defense article,” where there would be modification to any of the items, the Department believes such assistance would inherently require the use of “technical data.” Therefore, this exclusion would be unacceptably broad. However, the Department has accepted the recommendation to clarify the definition and exclude changes to fit to any of the items involved in the integration activity, provided that such services do not entail the use of “technical data” directly related to the “defense article.” Upon review, changes to fit are not an aspect of integration, which is the “engineering analysis needed to unite a ‘defense article’ and one or more items,” and therefore are not captured in paragraph (a)(2). The modifications of the “defense article” to accommodate the fit of the item to be integrated, which are within the activity covered by installation, are only those modifications to the “defense article” that allow the item to be placed in its predetermined location. Any modifications to the design of a “defense article” are beyond the scope of installation. Additionally, while minor modifications may be made to a “defense article” without the activity being controlled under (a)(2) as an integration activity, all modifications of defense articles, regardless of sophistication, are activities controlled under (a)(1) if performed by someone with prior knowledge of U.S.-origin “technical data.” “Fit” is defined in ITAR § 120.41: “The fit of a commodity is defined by its ability to physically interface or connect with or become an integral part of another commodity” (*see*, Note 4 to paragraph (b)(3)).

Commenting parties recommended revising paragraph (a)(2) to provide that such assistance described therein would be a “defense service” only if U.S.-origin “technical data” is exported. The law and regulations do not mandate this limitation. Section 38 of the Arms Export Control Act provides that the President is authorized to control the “export” of defense articles and defense services. The ITAR, in defining “defense article,” “technical data,” and “export,” does not provide the qualifier “U.S.-

origin” (see ITAR §§ 120.6, 120.10, and 120.17, respectively). In the instance described by the commenting party, of the integration of a commercial item into a foreign-origin “defense article,” the Department retains jurisdiction when the service is provided by a U.S. person.

A commenting party recommended revising paragraph (a)(2) so that the paragraph (a)(1) exception of the furnishing of assistance using “public domain” information is not nullified by paragraph (a)(2), as most of the activities described in paragraph (a)(1) involve integration as defined in the note to paragraph (a)(2). The Department believes each of the activities described in paragraphs (a)(1) and (a)(2) are sufficiently well defined to distinguish them one from the other. Therefore, the Department does not agree that paragraph (a)(2) nullifies the intention of paragraph (a)(1), and does not accept this recommendation.

A commenting party requested clarification that providing an item subject to the EAR for the purposes of integration into a “defense article” is not a “defense service.” The provision of the item in this instance, unaccompanied by assistance in the integration of the item into a “defense article,” is not within the scope of “the furnishing of assistance,” and therefore is not a defense service.

Commenting parties recommended clarification on whether the servicing of an item subject to the EAR that has been integrated with a “defense article” would be a “defense service.” The Department notes that such activity is not a “defense service,” provides it as an example of what is not a “defense service” in the note to paragraph (a), and also notes that it would be incumbent on the applicant to ensure that in providing this service, “technical data” directly related to the “defense article” is not used.

Commenting parties expressed concern over the potential negative effect of paragraph (a)(2) and the definition in general on university-based educational activities and scientific communication, and recommended clarification of the relationship between the definition of “defense services” and the exemption for the “export” of “technical data” at ITAR § 125.4(b)(10). Disclosures of “technical data” to foreign persons who are bona-fide and full time regular employees of universities continue to be exports for which ITAR § 125.4(b)(10) is one licensing exemption. The Department believes that, in most cases, the normal duties of a university employee do not encompass the

furnishing of assistance to a foreign person, in the activities described in paragraph (a). Therefore, in the context of employment with the university, the Department does not perceive that the foreign person’s use of the “technical data” would be described by ITAR § 120.9(a)(2), or any part of paragraph (a).

In response to the recommendation of one commenting party, the Department added a note clarifying that the installation of an item into a “defense article” is not a “defense service,” provided no “technical data” is used in the rendering of the service.

A commenting party recommended clarification of the licensing process for the “export” of an EAR 600 series item that is to be integrated into a “defense article.” The Department of Commerce has “export” authority over the 600 series item, and the exporter must obtain a license from the Department of Commerce, if necessary. The exporter must also obtain an approval from the Department of State to provide any “defense service,” including integration assistance pursuant to paragraph (a)(2).

A commenting party recommended removing “testing” as a type of “defense service,” stating it was not included in the definition of “organizational-level maintenance.” In including testing as part of the former definition but not of the latter, the Department does not perceive an inconsistency or conflict. To the extent that certain testing is within the definition of organization-level maintenance, that testing is explicitly excluded, as organizational-level maintenance is not covered under the definition of a “defense service.” However, all other testing remains a “defense service.” The Department intends for the furnishing of assistance to a foreign person, whether in the United States or abroad, in the testing of defense articles to be an activity requiring Department approval under the conditions of paragraph (a)(1). The Department did not accept this recommendation.

Commenting parties provided recommendations for revising the definitions of “public domain” information and “technical data.” Those definitions are proposed in this rule as well. To the extent that evaluation of the proposed changes to “defense services” hinges on these terms, the Department invites commenting parties to submit analyses of the impact of these revised definitions on the revised “defense service” definition in this proposed rule.

Commenting parties recommended clarification of the regulation regarding the furnishing of assistance and training

in organizational-level (basic-level) maintenance. The Department harmonized paragraph (a)(1) and the example regarding organizational-level maintenance by revising the Note to Paragraph (a), which sets forth activities that are not “defense services,” so that it specifically provides that “the furnishing of assistance (including training) in organizational-level (basic-level) maintenance of a defense article” is an example of an activity that is not a defense service.

In response to commenting parties, the Department clarifies that the example of employment by a foreign person of a natural U.S. person as not constituting a “defense service” is meant to address, among other scenarios, the instance where such a person is employed by a foreign defense manufacturer, but whose employment in fact does not entail the furnishing of assistance as described in ITAR § 120.9(a). By “natural person,” the Department means a human being, as may be inferred from the definition of “person” provided in ITAR § 120.14.

In response to the recommendation of a commenting party, the Department confirms that, as stated in a Department of Commerce notice, “Technology subject to the EAR that is used with technical data subject to the ITAR that will be used under the terms of a Technical Assistance Agreement (TAA) or Manufacturing License Agreement (MLA) and that would otherwise require a license from [the Department of Commerce] may all be exported under the TAA or MLA” (see 78 FR 22660). In DDTC publication *Guidelines for Preparing Electronic Agreements (Revision 4.2)*, Section 20.1.d., the following conditions are stipulated: The technology subject to the EAR will be used with “technical data” subject to the ITAR and described in the agreement, and the technology subject to the EAR will be used under the terms of a TAA or MLA (see <http://www.pmddtc.state.gov/licensing/agreement.html>).

Request for Comments

The Department invites public comment on any of the proposed definitions set forth in this rulemaking. With respect to the revisions to ITAR § 120.17, the Department recognizes the increasingly complex nature of telecommunications infrastructure and the manner in which data is transmitted, stored, and accessed, and accordingly seeks public comment with special emphasis on: (1) How adequately the proposed regulations address the technical aspects of data transmission and storage; (2) whether

the proposed regulations mitigate unintended or unauthorized access to transmitted or stored data; and (3) whether the proposed regulations impose an undue financial or compliance burden on the public.

The public is also asked to comment on the effective date of the final rule. Export Control Reform rules that revised categories of the USML and created new 600 series ECCN have had a six-month delayed effective date to allow for exporters to update the classification of their items. In general, rules effecting export controls have been effective on the date of publication, due to the impact on national security and foreign policy. As this proposed rule and the companion proposed rule from the Bureau of Industry and Security revise definitions within the ITAR and the EAR and do not make any changes to the USML or CCL, the Department proposes (should the proposed rule be adopted) a 30-day delayed effective date to allow exporters to ensure continued compliance.

Regulatory Analysis and Notices

Administrative Procedure Act

The Department of State is of the opinion that controlling the import and export of defense articles and services is a foreign affairs function of the U.S. government and that rules implementing this function are exempt from sections 553 (rulemaking) and 554 (adjudications) of the Administrative Procedure Act (APA). Although the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of the APA, the Department is publishing this rule with a 60-day provision for public comment and without prejudice to its determination that controlling the import and export of defense services is a foreign affairs function.

Regulatory Flexibility Act

Since the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of 5 U.S.C. 553, there is no requirement for an analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This proposed amendment does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the

Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (the "Act"), a major rule is a rule that the Administrator of the OMB Office of Information and Regulatory Affairs finds has resulted or is likely to result in: (1) An annual effect on the economy of \$100,000,000 or more; (2) a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or (3) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets.

The Department does not believe this rulemaking will have an annual effect on the economy of \$100,000,000 or more, nor will it result in a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions, or have significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets. The proposed means of solving the issue of data protection are both familiar to and extensively used by the affected public in protecting sensitive information.

Executive Orders 12372 and 13132

This proposed amendment will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this proposed amendment does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this proposed amendment.

Executive Orders 12866 and 13563

Executive Orders 12866 and 13563 direct agencies to assess costs and benefits of available regulatory

alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). The executive orders stress the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This proposed rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the proposed rule has been reviewed by the Office of Management and Budget (OMB).

Executive Order 12988

The Department of State has reviewed the proposed amendment in light of sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department of State has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, Executive Order 13175 does not apply to this rulemaking.

Paperwork Reduction Act

This rule does not impose any new reporting or recordkeeping requirements subject to the Paperwork Reduction Act, 44 U.S.C. Chapter 35; however, the Department of State seeks public comment on any unforeseen potential for increased burden.

List of Subjects

22 CFR 120 and 125

Arms and munitions, Classified information, Exports.

22 CFR 123

Arms and munitions, Exports, Reporting and recordkeeping requirements.

22 CFR Part 127

Arms and munitions, Exports, Crime, Law, Penalties, Seizures and forfeitures.

Accordingly, for the reasons set forth above, title 22, chapter I, subchapter M, parts 120, 123, 125, and 127 are proposed to be amended as follows:

PART 120—PURPOSE AND DEFINITIONS

■ 1. The authority citation for part 120 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2794; 22 U.S.C. 2651a; Pub. L. 105–261, 112 Stat. 1920; Pub. L. 111–266; Section 1261, Pub. L. 112–239; E.O. 13637, 78 FR 16129.

■ 2. Section 120.6 is amended by designating the current text as paragraph (a), revising the first sentence of newly designated paragraph (a), and adding paragraph (b) to read as follows:

§ 120.6 Defense article.

(a) *Defense article* means any item, software, or technical data designated in § 121.1 of this subchapter. * * *

(b) The following are not defense articles and thus not subject to the ITAR:

- (1) [Reserved]
- (2) [Reserved]
- (3) Information and software that:
 - (i) Are in the public domain, as described in § 120.11;
 - (ii) Arise during, or result from, fundamental research, as described in § 120.46;
 - (iii) Concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution; or
 - (iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order.

Note to paragraph (b): Information that is not within the scope of the definition of technical data (see § 120.10) and not directly related to a defense article, or otherwise described on the USML, is not subject to the ITAR.

■ 3. Section 120.9 is revised to read as follows:

§ 120.9 Defense service.

(a) *Defense service* means:

- (1) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the production, assembly, testing, intermediate- or depot-level maintenance (see § 120.38), modification, demilitarization, destruction, or processing of a defense article (see § 120.6), by a U.S. person or foreign person in the United States, who has knowledge of U.S.-origin technical data directly related to the defense article that is the subject of the assistance, prior to performing the service;

Note 1 to paragraph (a)(1): “Knowledge of U.S.-origin technical data” for purposes of paragraph (a)(1) can be established based on all the facts and circumstances. However, a person is deemed to have “knowledge of

U.S.-origin technical data” directly related to a defense article if the person participated in the development of a defense article described in the same USML paragraph or accessed (physically or electronically) technical data directly related to the defense article that is the subject of the assistance, prior to performing the service.

Note 2 to paragraph (a)(1): U.S. persons abroad who only receive U.S.-origin technical data as a result of their activities on behalf of a foreign person are not included within paragraph (a)(1).

Note 3 to paragraph (a)(1): Foreign person employees in the United States providing defense services as part of Directorate of Defense Trade Controls-authorized employment need not be listed on the U.S. employer’s technical assistance agreement or receive separate authorization to perform defense services on behalf of their authorized U.S. employer.

(2) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the development of a defense article, or the integration of a defense article with any other item regardless of whether that item is subject to the ITAR or technical data is used;

Note to paragraph (a)(2): “Integration” means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software to enable operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from “installation.” Installation means the act of putting an item in its predetermined place without the use of technical data or any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, and there is no use of technical data.). The “fit” of an item is defined by its ability to physically interface or connect with or become an integral part of another item. (see § 120.41).

(3) The furnishing of assistance (including training) to a foreign person (see § 120.16), regardless of whether technical data is used, whether in the United States or abroad, in the employment of a defense article, other than basic operation of a defense article authorized by the U.S. government for export to the same recipient;

(4) Participating in or directing combat operations for a foreign person (see § 120.16), except as a member of the regular military forces of a foreign

nation by a U.S. person who has been drafted into such forces; or

(5) The furnishing of assistance (including training) to the government of a country listed in § 126.1 of this subchapter in the development, production, operation, installation, maintenance, repair, overhaul or refurbishing of a defense article or a part component, accessory or attachments specially designed for a defense article.

Note to paragraph (a): The following are examples of activities that are not defense services:

1. The furnishing of assistance (including training) in organizational-level (basic-level) maintenance (see § 120.38) of a defense article;
 2. Performance of services by a U.S. person in the employment of a foreign person, except as provided in this paragraph;
 3. Servicing of an item subject to the EAR (see § 120.42) that has been integrated or installed into a defense article, or the servicing of an item subject to the EAR into which a defense article has been installed or integrated, without the use of technical data, except as described in paragraph (a)(5) of this section;
 4. The installation of any item into a defense article, or the installation of a defense article into any item;
 5. Providing law enforcement, physical security, or personal protective services (including training and advice) to or for a foreign person (if such services necessitate the export of a defense article a license or other approval is required for the export of the defense article, and such services that entail the employment or training in the employment of a defense article are addressed in paragraph (a)(3) of this section);
 6. The furnishing of assistance by a foreign person not in the United States;
 7. The furnishing of medical, logistical (other than maintenance), translation, financial, legal, scheduling, or administrative services;
 8. The furnishing of assistance by a foreign government to a foreign person in the United States, pursuant to an arrangement with the Department of Defense; and
 9. The instruction in general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities.
- (b) [Reserved]

■ 4. Section 120.10 is revised to read as follows:

§ 120.10 Technical data.

(a) *Technical data* means, except as set forth in paragraph (b) of this section:

- (1) Information required for the development (see § 120.47) (including design, modification, and integration design), production (see § 120.48) (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article. Technical data may be in any tangible or intangible form, such as written or

oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;

Note to paragraph (a)(1): The modification of an existing item creates a new item and technical data for the modification is technical data for the development of the new item.

(2) Information enumerated on the USML (*i.e.*, not controlled pursuant to a catch-all USML paragraph);

(3) Classified information for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article or a 600 series item subject to the EAR;

(4) Information covered by an invention secrecy order; or

(5) Information, such as decryption keys, network access codes, or passwords, that would allow access to other technical data in clear text or software (*see* § 127.1(b)(4) of this subchapter).

(b) *Technical data does not include:*

(1) Non-proprietary general system descriptions;

(2) Information on basic function or purpose of an item; or

(3) Telemetry data as defined in note 3 to USML Category XV(f) (*see* § 121.1 of this subchapter).

■ 5. Section 120.11 is revised to read as follows:

§ 120.11 Public domain.

(a) Except as set forth in paragraph (b) of this section, unclassified information and software are in the public domain, and are thus not technical data or software subject to the ITAR, when they have been made available to the public without restrictions upon their further dissemination such as through any of the following:

(1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;

(2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;

(3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;

(4) Public dissemination (*i.e.*, unlimited distribution) in any form (*e.g.*, not necessarily in published form), including posting on the Internet on sites available to the public; or

(5) Submission of a written composition, manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for publication or presentation.

(b) Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from:

(1) The Directorate of Defense Trade Controls;

(2) The Department of Defense's Office of Security Review;

(3) The relevant U.S. government contracting entity with authority to allow the technical data or software to be made available to the public; or

(4) Another U.S. government official with authority to allow the technical data or software to be made available to the public.

Note 1 to § 120.11: Section 127.1(a)(6) of this subchapter prohibits, without written authorization from the Directorate of Defense Trade Controls, U.S. and foreign persons from exporting, reexporting, retransferring, or otherwise making available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in paragraph (b) of this section.

Note 2 to § 120.11: An export, reexport, or retransfer of technical data or software that was made publicly available by another person without authorization is not a violation of this subchapter, except as described in § 127.1(a)(6) of this subchapter.

■ 6. Section 120.17 is revised to read as follows:

§ 120.17 Export.

(a) Except as set forth in § 120.52, § 126.16, or § 126.17 of this subchapter, *export* means:

(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article outside of the United States in any manner;

(2) Releasing or otherwise transferring technical data or software (source code or object code) to a foreign person in the United States (a "deemed export");

(3) Transferring by a person in the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person;

(4) Releasing or otherwise transferring a defense article to an embassy or to any

agency or subdivision of a foreign government, such as a diplomatic mission, in the United States;

(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad;

(6) Releasing or otherwise transferring information, such as decryption keys, network access codes, passwords, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred; or

(7) Making technical data available via a publicly available network (*e.g.*, the Internet).

(b) Any release in the United States of technical data or software to a foreign person is a deemed export to all countries in which the foreign person has held citizenship or holds permanent residency.

■ 7. Section 120.19 is revised to read as follows:

§ 120.19 Reexport.

(a) Except as set forth in § 120.52, *reexport* means:

(1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;

(2) Releasing or otherwise transferring technical data or software to a foreign person of a country other than the foreign country where the release or transfer takes place (a "deemed reexport");

(3) Transferring by a person outside of the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person outside the United States; or

(4) Releasing or otherwise transferring outside of the United States information, such as decryption keys, network access codes, password, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred.

(b) [Reserved]

§ 120.41 [Amended]

■ 8. Section 120.41 is amended by reserving Note 1 to paragraph (b)(3) and Note 2 to paragraph (b)(3).

■ 9. Section 120.46 is added to read as follows:

§ 120.46 Required.

(a) As applied to technical data, the term *required* refers to only that portion

of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required technical data may be shared by different products.

Note 1 to paragraph (a): The references to “characteristics” and “functions” are not limited to entries on the USML that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. For example, USML Category VIII(a)(1) controls aircraft that are “bombers.” No performance level is identified in the entry, but the characteristic of the aircraft that is controlled is that it is a bomber. Thus, any technical data, regardless of significance, peculiar to making an aircraft a bomber as opposed to, for example, an aircraft controlled under ECCN 9A610.a or ECCN 9A991.a, would be technical data required for a bomber and thus controlled under USML Category VIII(i).

Note 2 to paragraph (a): The ITAR and the EAR often divide within each set of regulations or between each set of regulations:

1. Controls on parts, components, accessories, attachments, and software; and
2. Controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated.

With the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data is the same as the jurisdictional status of the defense article or item subject to the EAR to which it is directly related. Thus, if technology is directly related to the production of an ECCN 9A610.x aircraft component that is to be integrated or installed in a USML Category VIII(a) aircraft, the technology is controlled under ECCN 9E610, not USML Category VIII(i).

Note 3 to paragraph (a): Technical data is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions” if it is used in or for use in the development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article unless:

1. The Department of State has determined otherwise in a commodity jurisdiction determination;
2. [Reserved];
3. It is identical to information used in or with a commodity or software that:
 - i. Is or was in production (*i.e.*, not in development); and
 - ii. Is not a defense article;
4. It was or is being developed with knowledge that it is for or would be for use in or with both defense articles and commodities not on the U.S. Munitions List; or

5. It was or is being developed for use in or with general purpose commodities or software (*i.e.*, with no knowledge that it would be for use in or with a particular commodity).

(b) [Reserved]

■ 10. Section 120.47 is added to read as follows:

§ 120.47 Development.

Development is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. Development includes modification of the design of an existing item.

■ 11. Section 120.48 is added to read as follows:

§ 120.48 Production.

Production means all production stages, such as product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance. This includes “serial production” where commodities have passed production readiness testing (*i.e.*, an approved, standardized design ready for large scale production) and have been or are being produced on an assembly line for multiple commodities using the approved, standardized design.

■ 12. Section 120.49 is added to read as follows:

§ 120.49 Technical data that arises during, or results from, fundamental research.

(a) *Technical Data arising during, or resulting from, fundamental research.* Unclassified information that arises during, or results from, fundamental research and is intended to be published is not technical data when the research is:

- (1) Conducted in the United States at an accredited institution of higher learning located; or
- (2) Funded, in whole or in part, by the U.S. government.

Note 1 to paragraph (a): The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technical data that arises during or results from fundamental research” except to the extent that such inputs are technical data that arose during or resulted from earlier fundamental research.

Note 2 to paragraph (a): There are instances in the conduct of research, whether fundamental, basic, or applied, where a researcher, institution, or company may decide to restrict or protect the release or publication of technical data contained in research results. Once a decision is made to

maintain such technical data as restricted or proprietary, the technical data becomes subject to the ITAR.

(b) *Prepublication review.* Technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data contained in the research without any restriction or delay, including U.S. government-imposed access and dissemination controls or research sponsor proprietary information review.

Note 1 to paragraph (b): Although technical data arising during or resulting from fundamental research is not considered “intended to be published” if researchers accept restrictions on its publication, such technical data will nonetheless qualify as technical data arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

Note 2 to paragraph (b): Research that is voluntarily subjected to U.S. government prepublication review is considered intended to be published for all releases consistent with any resulting controls.

Note 3 to paragraph (b): Technical data resulting from U.S. government funded research which is subject to government-imposed access and dissemination or other specific national security controls qualifies as technical data resulting from fundamental research, provided that all government-imposed national security controls have been satisfied.

(c) *Fundamental research definition.* Fundamental research means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

(1) *Basic research* means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

(2) *Applied research* means the effort that:

(i) Normally follows basic research, but may not be severable from the related basic research;

(ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and

(iii) Attempts to advance the state of the art.

■ 13. Section 120.50 is added to read as follows:

§ 120.50 Release.

(a) Except as set forth in § 120.52, technical data and software are released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data or software to a foreign person; or

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad.

(b) [Reserved]

■ 14. Section 120.51 is added to read as follows:

§ 120.51 Retransfer.

Except as set forth in § 120.52 of this subchapter, a *retransfer* is a change in end use or end user of a defense article within the same foreign country.

■ 15. Section 120.52 is added to read as follows:

§ 120.52 Activities that are not exports, reexports, or retransfers.

(a) The following activities are not exports, reexports, or retransfers:

(1) Launching a spacecraft, launch vehicle, payload, or other item into space;

(2) While in the United States, releasing technical data or software to a U.S. person;

(3) Shipping, moving, or transferring defense articles between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census; and

(4) Sending, taking, or storing technical data or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications; and

(iv) Not stored in a country proscribed in § 126.1 of this subchapter or the Russian Federation.

(b) For purposes of this section, end-to-end encryption means the provision of uninterrupted cryptographic

protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access technical data or software in encrypted form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such technical data or software.

Note to § 120.52: See § 127.1 of this subchapter for prohibitions on the release or transfer of technical data or software, in any form, to any person with knowledge that a violation will occur.

PART 123—LICENSES FOR THE EXPORT AND TEMPORARY IMPORT OF DEFENSE ARTICLES

■ 16. The authority citation for part 123 continues to read as follows:

Authority: Secs. 2, 38, and 71, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2753; 22 U.S.C. 2651a; 22 U.S.C. 2776; Pub. L. 105–261, 112 Stat. 1920; Sec. 1205(a), Pub. L. 107–228; Section 1261, Pub. L. 112–239; E.O. 13637, 78 FR 16129.

■ 17. Section 123.28 is added to read as follows:

§ 123.28 Scope of a license.

Unless limited by a condition set out in a license, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. DDTC grants licenses in reliance on representations the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted.

PART 124—AGREEMENTS, OFF-SHORE PROCUREMENT, AND OTHER DEFENSE SERVICES

■ 18. The authority citation for part 124 continues to read as follows:

Authority: Secs. 2, 38, and 71, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; 22 U.S.C. 2776; Section 1514, Pub. L. 105–261; Pub. L. 111–266; Section 1261, Pub. L. 112–239; E.O. 13637, 78 FR 16129.

■ 19. Section 124.1 is amended by adding paragraph (e) to read as follows:

§ 124.1 Manufacturing license agreements and technical assistance agreements.

* * * * *

(e) Unless limited by a condition set out in an agreement, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the agreement, license, and any letters of explanation. DDTC approves agreements and grants licenses in reliance on representations the applicant made in or submitted in connection with the agreement, letters of explanation, and other documents submitted.

PART 125—LICENSES FOR THE EXPORT OF TECHNICAL DATA AND CLASSIFIED DEFENSE ARTICLES

■ 20. The authority citation for part 125 continues to read as follows:

Authority: Secs. 2 and 38, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778); 22 U.S.C. 2651a; E.O. 13637, 78 FR 16129.

■ 21. Section 125.4 is amended by revising paragraph (b)(9) to read as follows:

§ 125.4 Exemptions of general applicability.

* * * * *

(b) * * *

(9) Technical data, including classified information, regardless of media or format, exported by or to a U.S. person or a foreign person employee of a U.S. person, travelling or on temporary assignment abroad subject to the following restrictions:

(i) Foreign persons may only export or receive such technical data as they are authorized to receive through a separate license or other approval.

(ii) The technical data exported under this authorization is to be possessed or used solely by a U.S. person or authorized foreign person and sufficient security precautions must be taken to prevent the unauthorized release of the technology. Such security precautions include encryption of the technical data, the use of secure network connections, such as virtual private networks, the use of passwords or other access restrictions on the electronic device or media on which the technical data is stored, and the use of firewalls and other network security measures to prevent unauthorized access.

(iii) The U.S. person is an employee of the U.S. government or is directly employed by a U.S. person and not by a foreign subsidiary.

(iv) Technical data authorized under this exception may not be used for foreign production purposes or for defense services unless authorized through a license or other approval.

(v) The U.S. employer of foreign persons must document the use of this exemption by foreign person employees,

including the reason that the technical data is needed by the foreign person for their temporary business activities abroad on behalf of the U.S. person.

(vi) Classified information is sent or taken outside the United States in accordance with the requirements of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case such guidance must be followed).

* * * * *

PART 127—VIOLATIONS AND PENALTIES

■ 22. The authority citation for part 127 continues to read as follows:

Authority: Sections 2, 38, and 42, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2791); 22 U.S.C. 401; 22 U.S.C. 2651a; 22 U.S.C. 2779a; 22 U.S.C. 2780; E.O. 13637, 78 FR 16129.

■ 23. Section 127.1 is amended by adding paragraphs (a)(6) and (b)(4) to read as follows:

§ 127.1 Violations.

(a) * * *

(6) To export, reexport, retransfer, or otherwise make available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in § 120.11(b) of this subchapter.

(b) * * *

(4) To release or otherwise transfer information, such as decryption keys, network access codes, or passwords, that would allow access to other technical data in clear text or to software that will result, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software. Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software.

* * * * *

Dated: May 20, 2015.

Rose E. Gottemoeller,

Under Secretary, Arms Control and International Security, Department of State.

[FR Doc. 2015-12844 Filed 6-2-15; 8:45 am]

BILLING CODE 4710-25-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

24 CFR Parts 91 and 576

[Docket No. FR-5474-N-02]

RIN 2506-AC29

Emergency Solutions Grants (ESG) Program, Solicitation of Comment on Specific Issues

AGENCY: Office of the Assistant Secretary for Community Planning and Development, HUD.

ACTION: Regulatory review; request for comments.

SUMMARY: On December 5, 2011, HUD published an interim rule entitled “Homeless Emergency Assistance and Rapid Transition to Housing: Emergency Solutions Grants Program and Consolidated Plan Conforming Amendments” (interim rule). The comment period for the interim rule ended on February 3, 2012. Because recipients and subrecipients have now had more experience implementing the interim rule, HUD recognizes that they may have additional input and comments for HUD to consider in its development of the ESG final rule (final rule). Therefore, this document takes comments for 60 days to allow additional time for public input, and for HUD to solicit specific comment on certain issues.

DATES: *Comment due date:* August 3, 2015.

ADDRESSES: Interested persons are invited to submit comments responsive to this request for information to the Regulations Division, Office of General Counsel, Department of Housing and Urban Development, 451 7th Street SW., Room 10276, Washington, DC 20410-7000. Communications must refer to the above docket number and title and should contain the information specified in the “Request for Comments” of this notice.

Electronic Submission of Comments.

Interested persons may submit comments electronically through the Federal eRulemaking Portal at <http://www.regulations.gov>. HUD strongly encourages commenters to submit comments electronically. Electronic submission of comments allows the commenter maximum time to prepare and submit a comment, ensures timely receipt by HUD, and enables HUD to make them immediately available to the public. Comments submitted electronically through the <http://www.regulations.gov> Web site can be viewed by interested members of the public. Commenters should follow

instructions provided on that site to submit comments electronically.

Submission of Hard Copy Comments. Comments may be submitted by mail or hand delivery. To ensure that the information is fully considered by all of the reviewers, each commenter submitting hard copy comments, by mail or hand delivery, should submit comments or requests to the address above, addressed to the attention of the Regulations Division. Due to security measures at all federal agencies, submission of comments or requests by mail often result in delayed delivery. To ensure timely receipt of comments, HUD recommends that any comments submitted by mail be submitted at least 2 weeks in advance of the public comment deadline. All hard copy comments received by mail or hand delivery are a part of the public record and will be posted to <http://www.regulations.gov> without change.

Note: To receive consideration as public comments, comments must be submitted through one of the two methods specified above. Again, all submissions must refer to the docket number and title of the rule.

No Facsimile Comments. Facsimile (fax) comments are not acceptable.

Public Inspection of Comments. All comments submitted to HUD regarding this notice will be available, without charge, for public inspection and copying between 8 a.m. and 5 p.m. weekdays at the above address. Due to security measures at the HUD Headquarters building, an advance appointment to review the documents must be scheduled by calling the Regulation Division at 202-708-3055 (this is not a toll-free number). Copies of all comments submitted will also be available for inspection and downloading at <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

Norm Suchar, Director, Office of Special Needs Assistance Programs, Office of Community Planning and Development, Department of Housing and Urban Development, 451 7th Street SW., Room 7262, Washington, DC 20410-7000, telephone number (202) 708-4300 (this is not a toll-free number). Persons with hearing or speech impairments may access this number through TTY by calling the toll-free Federal Relay Service at 800-877-8339.

SUPPLEMENTARY INFORMATION:

THE 1ST AMENDMENT, 2ND AMENDMENT, AND 3D PRINTED GUNS

JOSH BLACKMAN*

We are standing at the dawn of the next great industrial revolution. With 3D printers people can print an infinite number of personalized and customized “things.” However, one manifestation of this bold new technology threatens to cast a specter on innovation: 3D printed guns. This Article explores how efforts to regulate, or even ban 3D guns, must satisfy constitutional scrutiny under both the First and Second Amendments.

The Second Amendment right to keep and bear arms includes a subsidiary right to acquire arms—what else are you going to keep and bear—which covers both the buyer, and seller in the transaction. Further, the seller has to obtain guns, including newly manufactured firearms. Thus, the Second Amendment supply chain protects a right to make arms. These constitutional guarantees preserve the right to acquire and make firearms, by 3D printer or other means.

Prohibitions on sharing and receiving information about 3D guns, in the form of CAD source code files, violate the First Amendment right to free speech. The fact that information about 3D guns is distributed in electronic format does not shield it from the Bill of Rights. Further, the “hybrid” First and Second Amendment right offers heightened constitutional protections when the government attempts to restrict speech about the right to keep and bear arms.

This Article concludes by offering a preliminary analysis of several proposals to regulate 3D guns. First, laws that prohibit the manufacturing and possession of 3D guns, without a showing that the weapons are highly dangerous, would likely be unconstitutional. Second, bans on individuals making and possessing 3D guns for personal use would represent an unprecedented expansion of gun control laws, as there are virtually no regulations on homemade firearms. Third, the application of the International Traffic in Arms Regulation (“ITAR”), designed to keep dangerous weapons and munitions out of the hands of foreign nationals is an ill-equipped, and as applied unconstitutional means to regulate 3D guns.

* Assistant Professor, South Texas College of Law. I would like to thank Brannon Denning, David Koppel, Steven Halbrook, Michael O'Shea, Glenn Harlan Reynolds, and David Wolitz.

INTRODUCTION.....	481
I. 3D PRINTED GUNS.....	483
A. <i>3D Printing</i>	483
B. <i>The Liberator</i>	485
C. <i>The Problem of 3D Guns</i>	486
II. THE RIGHT TO BEAR, ACQUIRE, AND MAKE ARMS	490
A. <i>The Right to Acquire Arms</i>	491
B. <i>The Right to Make Arms</i>	496
III. THE FIRST AMENDMENT AND 3D-PRINTED GUNS	498
A. <i>Information is Speech</i>	498
B. <i>The Right to Create and Disseminate Information</i>	502
IV. THE HYBRID FIRST AND SECOND AMENDMENTS.....	504
V. THE REGULATION OF 3D GUNS.....	507
A. <i>Bans on Manufacturing and Possession of 3D-Printed Guns</i>	508
B. <i>Bans on Materials Used For Printing 3D Guns</i>	512
C. <i>Intellectual Property Regulations and 3D-Printed Guns</i>	513
1. Filtering CAD Files on the internet	515
2. Digital Rights Management on 3D Printers.....	517
3. Digital Millennium Patent Act	520
D. <i>Export Controls of Information about 3D Guns</i>	522
1. ITAR and the First Amendment.....	522
a. <i>Karn v. United States Department of State</i>	524
b. <i>Bernstein v. U.S. Department of Justice</i>	526
c. <i>Junger v. Daley</i>	528
2. Unliberating the Liberator.....	530
3. The Constitutionality of ITAR as Applied to 3D Guns	531
a. <i>ITAR as Content-Based Prior Restraint of Speech</i>	531
b. <i>Balancing National Security and the First and Second Amendments</i>	535
c. <i>The Regulation of Information</i>	536
CONCLUSION	537

INTRODUCTION

We are standing at the dawn of the next great industrial revolution. Three-dimensional printing transforms designs on a computer into three-dimensional objects of all shapes and sizes. From the convenience of home, people can print an infinite number of personalized and customized “things.” However, one manifestation of this bold new technology threatens to cast a specter on innovation: 3D printed guns. This Article explores how efforts to regulate, or even ban 3D guns, must satisfy constitutional scrutiny under both the First and Second Amendments.

Part I explains how 3D printers can transform computer source code—which describes the shapes and position of virtual objects—into actual, three-dimensional objects. Perhaps the most notorious object has been the Liberator, a handgun manufactured entirely out of plastic parts created by a 3D printer. Concerns about 3D printed guns have been vastly overstated. Under existing law, it is perfectly legal to personally manufacture a firearm, without any need to register it, or seek permission of the government. Further, with supplies available at any hardware store, it is quite simple to cheaply build an undetectable, lethal weapon out of non-metal parts. In addition, for the foreseeable future, it is exponentially more expensive and time consuming to build a gun with a 3D printer. These fears should not drive a broader debate about regulation of this new innovative technology.

Part II places the individual right to keep and bear arms, as recognized in *District of Columbia v. Heller*, in the context of its two subsidiary rights: acquiring and making arms. First, before one can keep and bear arms, as the Constitution guarantees, one has to obtain the gun from somewhere. Thus, any meaningful Second Amendment right encompasses the *right to acquire arms*. This right can be reasonably regulated, but not banned. The right to acquire arms must offer constitutional protection for both participants in the transaction—the buyer and the seller. Again, these rights can be reasonably limited, but not banned. Second, the seller of the gun has to be able to obtain the gun from somewhere to resell it—either acquiring a used gun, or, through making a new gun. Both of these sources in the Second Amendment supply chain must be protected, and subject to constitutional scrutiny. The latter represents the *right to make arms*, which can also be reasonably regulated but not banned. The right to make arms for personal use, more so than commercial manufacturing, historically has been subject to virtually no regulations. It is deeply rooted in our nation’s history and traditions. The Second Amendment, consistent with *Heller*, protects three guarantees: the right to keep and bear arms, the right to

acquire arms (for both the buyer and seller), and the right to make arms.

Part III considers the intersection of the First Amendment and the sharing and receiving of information about 3D guns. If Congress banned a book discussing how to build a handgun, which includes detailed blueprints and schematics of how the pieces should be assembled, it would be facially unconstitutional as a content-based prior restraint of speech. But what if Congress prohibited the same information, except rather than being printed on paper, it is shared in a digital format? This approach—how some propose stopping 3D guns—would similarly violate the freedom of speech. The Supreme Court has made clear that information, regardless of its format—whether books or movies or video games or electronic data—is protected speech. The 3D computer-aided design (“CAD”) files used to describe and create 3D printed objects fit within this category of expressive information. Bans on these blueprints achieve neither the compelling state interest, nor are sufficiently narrowly tailored, to survive constitutional scrutiny. Further, the Supreme Court has found that the right of freedom of speech includes not only the rights of the speaker, but also of the public to receive that information. Restrictions on the ability to share 3D blueprints chill not only the constitutional rights of the teachers who shares that information, but also of the students who wish to learn. For these reasons, bans on 3D blueprints would violate the First Amendment.

Part IV introduces the concept of the *hybrid* First and Second Amendments right. These complimentary rights work together in tandem to bolster constitutional protections when the government attempts to restrict speech about the right to keep and bear arms. The Supreme Court has found that the freedom of speech is instrumental in promoting other constitutional guarantees, such as the freedom of religion, the freedom of association, the right to a public trial, and others. When one constitutional right reinforces another, the government bears a stronger burden to infringe individual liberty. The hybrid approach lends itself well to the context of 3D printed guns. Prohibitions on 3D gun blueprints would violate not only the First and Second Amendment standing by themselves, but also both guarantees working together in tandem. Efforts to stop the sharing, and receipt of this information, would impose a greater burden on the government to justify limiting two of our most fundamental constitutional guarantees. In this sense, the right to design, make, and share information about 3D guns is even more protected by the freedom of speech *and* the right to keep and bear arms.

Part V offers a preliminary analysis of several proposals to regulate 3D guns. First, laws that prohibit the manufacturing and possession of 3D guns, without a showing that the weapons are

highly dangerous, would likely be unconstitutional. Further, bans on individuals making and possessing 3D guns for personal use would represent an unprecedented expansion of gun control laws, as there are virtually no regulations on homemade firearms. However, the commercial sale of firearms, manufactured by 3D printers or otherwise, could be reasonably regulated in manners consistent with the current sale of traditional firearms. Second, efforts to regulate the supplies used to make 3D guns, whether the plastic polymers used in the printing process, or gunpowder for bullets would be an undue burden placed before the right to make arms. Further it would broadly chill speech by limiting what innovations, other than guns, can be created with 3D printers. Finally, the application of the International Traffic in Arms Regulation (“ITAR”), designed to keep dangerous weapons and munitions out of the hands of foreign nationals, represents an unconstitutional effort to chill speech, and censor information about the right to keep and bear arms. As applied to the Liberator, an open-sourced handgun—the quintessential weapon protected in *Heller*—international arms regulations are an ill-equipped, and as applied unconstitutional means to regulate 3D guns.

In the final analysis, 3D printers may lead to a renaissance of innovation. The government should tread carefully in restricting this technology to protect intellectual property. However, this prudential concern is transformed into a constitutional violation when efforts to infringe on this technology trample on the First and Second Amendments. Let technology and our constitutional rights be free.¹

I. 3D PRINTED GUNS

A. 3D Printing

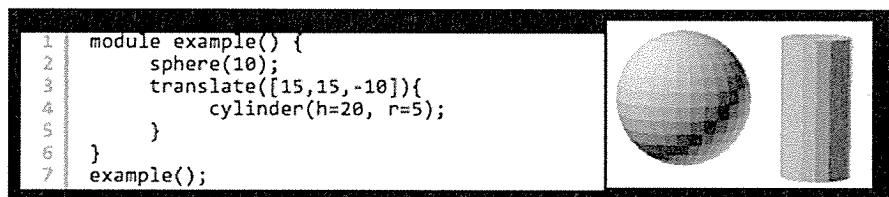
3D Printing, also known as “additive manufacturing,” is a process where a three-dimensional model designed on a computer is transformed into a three-dimensional solid object. 3D Printing holds great potential to transform the way manufacturing works. During his February 2013 State of the Union address, President Obama said 3D printing “has the potential to revolutionize the way we make almost everything.”²

1. See generally ORLY LOBEL, TALENT WANTS TO BE FREE (2014).

2. Office of the Press Secretary, *Remarks by the President in the State of the Union Address*, WHITE HOUSE (Feb. 12, 2013 9:15 PM), <http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address>.

3D printers, much like desktop printers, “employ an additive process, which involves squirting molten plastic, targeting a laser to harden layers of powder or liquid resin, or shaping other materials such as metal, cake frosting, or living cells, to make an object.”³ Through this process, “raw material is set into two-dimensional patterns on a platform that is gradually raised to let each layer stack on top of the next until the item is complete.”⁴ The designs for these three-dimensional objects are controlled by a Computer-Aided Design (“CAD”) files that use source code, much like other object-oriented programming languages, to define the shapes, sizes, and positions of three-dimensional objects.

For example, here is the source code for a very simple 3D CAD file creating two three-dimensional objects, a sphere and a cylinder.⁵



The source code consists of seven lines. Each line is numbered to the left of the column. First, the code on line 2 generates a sphere with a radius of 10. Second, the code on line 4 generates a cylinder with a height of 20 and a radius of 5. The code on line three spaces, or “translates,” the two shapes apart from each other—it is moved 15 units to the right on the x-axis, 15 units to the right on the y-axis, and 10 units back on the z-axis (this is the third dimension). When viewed with perspective, the cylinder appears behind the sphere, lower, and to the right.

3. Deven R. Desai & Gerard N. Magliocca, *Patents, Meet Napster: 3D Printing and the Digitization of Things*, 102 GEO. L.J. (forthcoming 2014) (manuscript at 9), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2338067; see also Bill Bumgarner, *Getting Started with a 3D Printer*, MAKE:, Winter 2013, at 12. (“There are three approaches to additive manufacturing in common use: *photopolymerization* (using light to cure a liquid material into solids of the desired shape), *granular materials binding* (using lasers, hot air, or other energy sources to fuse layers of powder into the desired shape), and the focus of this article, *molten polymer deposition* (MPD; extruding molten material in layers to build up the desired shape).”).

4. Desai & Magliocca, *supra* note 3 (manuscript at 9).

5. Brian Benchoff, *3D Printer: Making a Thing with OpenSCAD*, HACKADAY (Dec. 11, 2013), <http://hackaday.com/2013/12/11/3d-printer-making-a-thing-with-openscad/>.

How are the 3D objects generated? This CAD file source code is “compiled,” with a software compiler, which generates object code. This machine-readable object code will be transformed into the 3D shapes viewed on the right. Further, that machine-readable code—incomprehensible to humans, but understandable by computers—is transmitted to a 3D printer, which will create the object using the additive manufacturing process.

Though in its present form 3D printing is fairly time-intensive, expensive, and limited in what it can create, “[t]he promise of 3D printing is that people will be free to make almost anything they want themselves, which opens the door to a new wave of innovation from the home, the start-up, and large firms.”⁶

B. *The Liberator*

While 3D printing has been used to create millions of different items, the creation of guns using additive manufacturing has generated vast amounts of controversy. The Wiki Weapons project, as it was then known, was able to create the plastic lower receiver for an AR-15 rifle from a 3D printer.⁷ Initial versions fell apart after firing six shots.⁸ Yet, later versions were able to fire six-hundred rounds successfully.⁹

The (aptly named) Liberator was the first handgun manufactured entirely from a parts created by a 3D printer.¹⁰ It was designed by former-law student Cody Wilson, who created the organization Defense Distributed.¹¹ The Liberator consists of twelve separate parts of “acrylonitrile butadiene styrene thermoplastic polymer,” with a single metal part—the firing pin.¹² Wilson posted

6. Desai & Magliocca, *supra* note 3 (manuscript at 3).

7. See Andy Greenberg, *Meet the “Liberator”: Test-Firing the World’s First Fully 3D-Printed Gun*, FORBES, (May 5, 2013, 5:30 PM), <http://www.forbes.com/sites/andygreenberg/2013/05/05/meet-the-liberator-test-firing-the-worlds-first-fully-3d-printed-gun/>.

8. *Printed Reinforced AR Lower Review*, WIKIWEP DEVBLOG (2013), <http://defdist.tumblr.com/post/37023487585/printed-reinforced-ar-lower-review>.

9. John Biggs, *Defense Distributed Prints an AR-15 Receiver that Has Fired More than 600 Rounds*, TECHCRUNCH (Mar. 1, 2013), <http://techcrunch.com/2013/03/01/defense-distributed-prints-an-ar-15-receiver-that-has-fired-more-than-600-rounds/>.

10. Greenberg, *supra* note 7.

11. *Id.*

12. Brian Doherty, *The Unstoppable Plastic Gun*, REASON.COM (Nov. 12, 2013, 7:00 AM), <http://reason.com/archives/2013/11/12/the-unstoppable-plastic-gun/print>.

the CAD files for the Liberator on the Defense Distributed Website on May 5, 2013, where they would remain for a few days.¹³ In a letter to Wilson dated May 8, 2013, the State Department asserted that the CAD files were regulated by export control laws, prohibiting the transmission of data about munitions to foreign nationals.¹⁴ Wilson immediately took down the website and the CAD files. By that point, nearly 100,000 people had downloaded the blueprint, and the files are still readily available on the internet.¹⁵

C. *The Problem of 3D Guns*

The Liberator unleashed a panic about the threat of 3D guns. Senator Chuck Schumer, who has proposed legislation that would ban 3D guns, sounded the alarm.¹⁶ “We’re facing a situation where anyone—a felon, a terrorist—can open a gun factory in their garage and the weapons they make will be undetectable. It’s stomach-churning.”¹⁷ The threat of the 3D guns, and the need for regulating them, has been *greatly* overstated.

Under federal law, it is legal to make pistols, revolvers, and rifles at home.¹⁸ For semi-automatic rifles, such as the AR-15, it is legal to make the lower receiver—the lower receiver is what makes a gun a “gun.”¹⁹ As long as the gun is not being sold, shared, or traded, no license is required.²⁰ The Bureau of Alcohol, Tobacco, Firearms, and Explosive (“BAFTE”) FAQ section explains, “[w]ith certain exceptions a firearm may be made by a non-licensee provided it is not for sale and the maker is not prohibited from possessing

13. *See id.*

14. Tim Worstall, *The “Liberator” Plastic Gun and the Export Regulations Take Down of It*, FORBES, (May 10, 2013, 8:54 AM), <http://www.forbes.com/sites/timworstall/2013/05/10/the-liberator-plastic-gun-and-the-export-regulations-take-down-of-it/>.

15. Doherty, *supra* note 12.

16. *See* Tim Murphy, *Chuck Schumer Wants to Stop You from Printing a Gun at Home. Good Luck.*, MOTHER JONES (May 8, 2013, 6:00 AM), <http://www.motherjones.com/politics/2013/05/chuck-schumer-defense-distributed-printed-gun>.

17. *Id.*

18. *General Questions*, U.S. DEPT OF JUST., BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, <http://www.atf.gov/firearms/faq/general.html> (last visited May 1, 2014).

19. Sebastian Anthony, *The World’s First 3D-Printed Gun*, EXTREMETECH (Jul. 26, 2013, 10:56 AM), <http://www.extremetech.com/extreme/133514-the-worlds-first-3d-printed-gun>.

20. *See General Questions*, *supra* note 18.

firearms.”²¹ The resulting gun need not be registered with BAFTE and is legal for use.²²

The simplest homemade guns are referred to as “zip guns.”²³ Building these improvised, cheap but dangerous firearms requires little expertise. One video on YouTube shows an improvised shotgun, which consists of two pieces of walled tubing, a nail, and a shotgun shell.²⁴ It cost \$7 of materials and took little time to make.²⁵ It is quite lethal, and will likely not set off a metal-detector.

While the notion of the homemade gun may make many uncomfortable, especially those unfamiliar with guns, this is not new technology. Columnist Brian Doherty observed that 3D printing brings a “change in convenience, not in kind; that people always had both the means and to some degree the legal right to arm themselves with homemade weapons.”²⁶ 3D printing does nothing to stop these types of weapons. In fact, for the foreseeable future, 3D guns will be much, much more difficult and expensive than zip guns or illegally procured (but readily available) firearms. Senator Schumer’s panic is unfounded. Using 3D printers to “open a gun factory in [a] garage”²⁷ would be an inefficient and expensive manner to create weapons that are undetectable.

Further, the fear of a factory spitting out pre-assembled weapons is fanciful. Contrary to Schumer suggestion, a working gun does not pop out of the 3D printer ready to fire, like a pop-tart from the toaster.²⁸ Using a 3D printer to create the parts, and assemble them, is a time-intensive process that requires advanced knowledge of machining and gunsmithing. In November of 2013, I visited Solid Concepts, a 3D printing firm in Austin, Texas. They manufactured

21. *Id.*

22. *See id.*

23. Philip Luty, *The “Zip Gun”*, HOMEGUNSMITH.COM, <http://thehomegunsmith.com/pdf/ZipGun.pdf> (last visited May 1, 2014).

24. Marksurbu, *\$7 12-Gauge Zip Gun Homemade Shotgun*, YOUTUBE (Sep. 23, 2010), <http://www.youtube.com/watch?v=n1wV3lmbSv4>.

25. *See id.*

26. Brian Doherty, *What 3D Printing Means for Gun Rights*, REASON.COM (Dec. 12, 2012), <http://reason.com/archives/2012/12/12/what-3-d-printing-means-for-gun-rights>.

27. Murphy, *supra* note 16.

28. Though if a Pop-Tart was chewed into the shape of a gun, Senator Schumer may want to ban that as well. *See* Deborah Hastings, *Boy, Suspended for Chewing Pop-Tart into Shape of Gun, Gets Lifetime NRA Membership*, N.Y. DAILY NEWS (May 31, 2013 3:10 PM), <http://www.nydailynews.com/news/national/boy-suspended-gun-shaped-pop-tart-lifetime-nra-membership-article-1.1359918>.

the first 3D-printed gun made out of metal.²⁹ The gun was an M1911, which was the standard issued sidearm for the United States army between 1911 and 1985.³⁰ Eric Mutchler, the project coordinator, told me that it took approximately a hundred hours to print all of the parts for the pistol.³¹ After all of the parts were printed, they needed to be finished, polished, and then assembled.³² Mutchler estimated the cost was roughly \$10,000 for a single gun.³³ These numerous assembly steps must be performed by someone with a deep knowledge of gunsmithing. This approach is not even remotely comparable to the assembly process used to cheaply manufacture firearms. Anyone who possesses these skills can much more easily make a gun at home using parts available from any hardware store.

Stated simply, bad people who want guns will find 3D printing a terrible mechanism of acquiring a gun. As one media account noted, “officials do not believe there’s a risk that street criminals will be able to mass produce guns using 3-D printing technology, as the printer required to produce a gun can cost more than \$100,000 and quality varies.”³⁴ The risk is not for “street criminals.”³⁵ David Kopel commented, “[t]he guy who is robbing a 7-Eleven isn’t going to buy a 3D printer.”³⁶ Cody Wilson, the creator of the Liberator, stated the obvious—“[3D] printing is a ridiculous way of making gun parts.”³⁷

29. See Cyrus Farivar, *Thought 3D-Printed Guns had to Be Made of Plastic? Think Again*, ARSTECHNICA (Nov. 7, 2013, 4:55 PM), <http://arstechnica.com/business/2013/11/thought-3d-printed-guns-had-to-be-made-of-plastic-think-again/>.

30. See *id.*

31. Josh Blackman, *Tour of 3D-Gun Printing Facility*, JOSH BLACKMAN’S BLOG (Nov. 12, 2013), <http://joshblackman.com/blog/2013/11/12/tour-of-3d-gun-printing-facility/>.

32. See *id.*

33. See *id.*

34. Holder Takes Aim at 3-D Guns, Calls for Renewal of Metal Detection Law, FOX NEWS (Nov. 15, 2013), <http://www.foxnews.com/us/2013/11/15/holder-says-3-d-guns-extremely-serious-problem-calls-on-congress-to-renew/>.

35. Devlin Barrett, *Threat of Plastic Guns Rises*, WALL ST. J. (Nov. 13, 2013, 9:34 PM), <http://online.wsj.com/news/articles/SB10001424052702303559504579196342767042548>.

36. Mark Gibbs, *The End of Gun Control*, FORBES (Jul. 28, 2012 4:24 PM), <http://www.forbes.com/sites/markgibbs/2012/07/28/the-end-of-gun-control/>.

37. Jennifer Preston, *Printable-Gun Instructions Spread Online After State Dept. Orders Their Removal*, N.Y. TIMES (May 10, 2013, 5:19 PM), <http://thelede.blogs.nytimes.com/2013/05/10/printable-gun-instructions-spread-online-after-state-dept-orders-their-removal/>.

A BAFTE official conceded as much, noting “This is more for someone who wants to get into an area and perhaps be an assassin. Or they want to go to a courthouse and shoot a witness.”³⁸ At the risk of sounding glib, creating undetectable guns, on a one-off basis, is much easier without a 3D printer. As the same official observed, plastic guns have been defeating security procedures, and “have been tried and true for the last 30 years,”³⁹ long before 3D printers existed. The apparent concern of these weapons is that they can be mass-produced by laymen—untrained assassins or perhaps amateur ninjas. There are so many better ways to obtain a gun more cheaply, easier, and without a paper trail, than to manufacture or buy a manufactured 3D gun.⁴⁰ The liberal magazine *Mother Jones* brings some calm to this panic: “[T]here are already upwards of 300 million nonplastic firearms currently in circulation in the United States, and they’re pretty easy to get a hold of. (It’s also already perfectly legal to make your gun from normal materials.)”⁴¹ The fear of 3D guns, therefore, is largely unfounded.

3D guns are not the only harmful items that can be created through 3D printing. “The ability to print . . . illicit drugs . . . suggests a dark side to 3D printing.”⁴² These negatives should not drive the broader debate over regulations of 3D printers. We should resist the urge to impose serious costs on a quickly moving industry out of an unrealistic fear of 3D guns. As one recent article notes, “[t]he danger is that these potential negatives will swamp the analysis and policy debates so that an incumbent or one sector gains an upper hand in demanding the hammer of the law stop certain technology.”⁴³ In many respects, regulations on 3D guns are gun

38. Barrett, *supra* note 35.

39. *Id.*

40. Paul M. Barrett, *Let’s All Calm Down About 3D Plastic Guns*, BUS. WK. (May 6, 2013), <http://www.businessweek.com/articles/2013-05-06/lets-all-calm-down-about-3-d-plastic-guns> (“Here’s why: If you’ve got the skills, you can already make a gun in your basement, and there are less complicated ways to do it than using a \$10,000 3D printer and computer set-up. Why would bad guys bother making comic book firearms when they can go online and order anything from a Glock 9 mm pistol to a Bushmaster military-style semiautomatic rifle with 30-round ammunition magazines? Perhaps the evil doer wouldn’t want to leave a credit-card trail. Then he pays cash at a Main Street gun shop, a weekend gun show, or to the criminal down the block who sells black market firepower from the trunk of his car. Or the crook steals or borrows his gun.”).

41. Murphy, *supra* note 16.

42. Desai & Magliocca, *supra* note 3 (manuscript at 18).

43. *Id.*

control solutions in search of a public safety problem. Putting aside policy arguments, however, efforts to regulate these guns will need to satisfy constitutional scrutiny under both the First and Second Amendments.

II. THE RIGHT TO BEAR, ACQUIRE, AND MAKE ARMS

The Second Amendment protects an individual right to keep and bear arms.⁴⁴ This right embodies two complimentary guarantees: the right to acquire arms, and the right to make arms. A meaningful right to keep and bear arms would require the preliminary steps of being able to create, and obtain guns. Without both of these two prerequisite incidents of the Second Amendment, the right to keep and bear arms would be quite hollow. What can you keep and bear if you cannot obtain arms made somewhere? Regulations limiting the manufacturing of guns with 3D printers will run into all three guarantees of the Second Amendment.

A right to sell arms must include a prerequisite that arms can be sold, which is the necessary consequence of a right to buy arms. Thus, it can be reasoned that the Second Amendment's right to bear arms, which is enabled by the right to sell arms, has at its base a right to make arms. While all three can be regulated, all three exist as necessary constitutional incidents of the Second Amendment, and they must adhere to constitutional scrutiny.⁴⁵

44. See *District of Columbia v. Heller*, 554 U.S. 570, 636 (2008) (“[T]he enshrinement of constitutional rights necessarily takes certain policy choices off the table. These include the absolute prohibition of handguns held and used for self-defense in the home. Undoubtedly some think that the Second Amendment is outmoded in a society where our standing army is the pride of our Nation, where well-trained police forces provide personal security, and where gun violence is a serious problem. That is perhaps debatable, but what is not debatable is that it is not the role of this Court to pronounce the Second Amendment extinct.”).

45. See David B. Kopel, *Does the Second Amendment Protect Firearms Commerce?*, 127 HARV. L. REV. F. 230 (2014), available at <http://harvardlawreview.org/2014/04/does-the-second-amendment-protect-firearms-commerce/> (“The *Heller* rule—that there is a qualified right to the commercial sale of arms—does not utterly forbid statutes governing non-commercial sales, gifts, or loans; but those statutes enjoy no presumption of constitutionality. They would have to be proven constitutional under some form of heightened scrutiny.”).

A. *The Right to Acquire Arms*

District of Columbia v. Heller recognized that the Second Amendment protects an individual right to keep and bear arms for purposes of self-defense.⁴⁶ The Supreme Court reaffirmed this right in *McDonald v. Chicago*, as applied to the states.⁴⁷ A thorough treatment of the Second Amendment, is far, far beyond the scope of this Article.⁴⁸ Since *McDonald*, the Supreme Court has consistently denied certiorari in every case implicating the Second Amendment.⁴⁹ As a result, the lower courts have split in many different ways, respecting the appropriate tier of scrutiny (intermediate or strict), who bears the burden of persuasion (the individual or the state), and the role that history plays in defining the right.⁵⁰

For purposes of 3D guns, one split in particular is salient. *Heller* did not address, directly at least, whether the Supreme Court protects the right to acquire arms. The ability to acquire arms requires, at a minimum, two parties—someone willing to buy the gun, and someone willing to sell the gun. Both are necessary conditions for any transaction. Thus, any right to acquire firearms would have to consider both the buyer and the seller—it takes two to tango. Protecting the right to buy, but banning the right to sell, would make a transaction impossible. Likewise, protecting the right to buy, but banning the right to sell, would not get you very far. Of course, each element could be regulated to different degrees, but the fact that neither can be banned entirely is a necessary consequence of the Second Amendment protecting this activity.

In *Heller*, the Supreme Court recognized that District of Columbia resident Dick Heller had the constitutional right to lawfully use a handgun.⁵¹ Or stated differently, the District of Columbia could not deny residents the ability to obtain, and register

46. See *id.*

47. See *McDonald v. Chicago*, 561 U.S. 742, 130 S.Ct. 3020, 3036 (2010).

48. For background on *Heller* and *McDonald*, see Ilya Shapiro & Josh Blackman, *Keeping Pandora's Box Sealed*, 8 GEO. J.L. & PUB. POL'Y 1 (2010); Alan Gura, Ilya Shapiro, & Josh Blackman, *The Tell-Tale Privileges or Immunities Clause*, 2010 CATO SUP. CT. REV. 163 (2010).

49. See Josh Blackman, *Our Gun-Shy Justices—The Supreme Court Abandons the Second Amendment*, AM. SPECTATOR, July 2014; Josh Blackman, *Cert. Denied in Lane v. Holder and NRA v. ATF*, JOSH BLACKMAN'S BLOG (Feb. 24, 2014), <http://joshblackman.com/blog/2014/02/24/cert-denied-in-lane-v-holder-and-nra-v-atf/>.

50. See generally David B. Kopel, *The First Amendment Guide to the Second Amendment*, 81 TENN. L. REV. 417 (2014).

51. See *Heller*, 554 U.S. at 592.

a firearm.⁵² The case was primarily about the right of Dick Heller, who owned his gun from before the District instituted its gun ban, to be able to legally keep and bear it for self-defense. Though, *Heller* did discuss, indirectly, the rights of sellers. Justice Scalia's majority opinion noted that the Second Amendment should not "cast doubt" on "laws imposing conditions and qualifications on the commercial sale of arms."⁵³ This mitigating language was intended to assuage concerns that the Second Amendment would now invalidate many laws on the books limiting the ability to buy and sell arms. However, this proviso does much more.

David Kopel reads this "exception [to] prove[] the rule. There is a right to the commercial sale of arms, but it is a right that may be regulated by 'conditions and qualifications.'"⁵⁴ In other words, if the "sale of arms" was not a constitutional right, it could be prohibited altogether under the police power, and not just limited by "conditions and qualifications." The need to qualify a right dictates the existence of the right in the first place. This operates in much the same way that noting that "laws forbidding the carrying of firearms *in sensitive places*" implies that there is a constitutional right to carry them in places that are not *sensitive*.⁵⁵ If it did not, carrying could be banned everywhere.

Following *Heller*, the Circuit Courts have split concerning whether the Second Amendment protects the right not only to bear arms, but also to acquire them. In an unpublished decision, the Fourth Circuit observed that nothing "remotely suggests that, at the time of its ratification, the Second Amendment was understood to protect an individual's right to *sell* a firearm."⁵⁶ In contrast, in *Ezell v. City of Chicago*, the Seventh Circuit found that a shooting range that sold ammunition and rented firearms successfully raised a claim under the Second Amendment on behalf of individuals who used the facility.⁵⁷ The court held that a Chicago law banning shooting ranges inside the city was very likely unconstitutional.⁵⁸ In its reasoning, the court stressed that the right to keep and bear arms

52. See *id.* at 628 ("The handgun ban amounts to a prohibition of an entire class of 'arms' that is overwhelmingly chosen by American society for that lawful purpose. The prohibition extends, moreover, to the home, where the need for defense of self, family, and property is most acute.").

53. *Id.* at 571.

54. Kopel, *supra* note 45.

55. *Id.*

56. *United States v. Chafin*, 423 F. App'x 342, 344 (4th Cir. 2011).

57. *Ezell v. City of Chicago*, 651 F.3d 684, 696–711 (7th Cir. 2011).

58. *Id.* at 710.

was burdened beyond an individual keeping and bearing arms: “The right to possess firearms for protection implies a *corresponding right to acquire and maintain* proficiency in their use; the core right wouldn’t mean much without the training and practice that make it effective.”⁵⁹ The key word is “acquire.”

After *Ezell*, a district court in Illinois found unconstitutional a ban on selling and acquiring firearms in Chicago city limits: “[The Second Amendment] right must also include the right to *acquire* a firearm.”⁶⁰ In light of *McDonald*, the court found invalid a law that “outright ban[ned] legal buyers and legal dealers from engaging in lawful acquisitions and lawful sales of firearms, [where] the evidence d[id] not support that the complete ban sufficiently further[ed] the purposes that the ordinance trie[d] to serve.”⁶¹ This reasoning is consistent with *Heller*’s implication about the unconstitutionality of a ban on firearms. The court reasoned, “[t]herefore, just as in *Ezell*, where the fact ‘[t]hat residents may travel outside the jurisdiction to fulfill the training requirement is irrelevant to the validity of the ordinance inside the City,’ so too here: the fact that Chicagoans may travel outside the City to acquire a firearm does not bear on the validity of the ordinance inside the City.”⁶²

David Kopel, observing the “developing” circuit split on the issue, has written that the “operating a business that provides Second Amendment services is protected by the Second Amendment,” in much the same way that the “First Amendment protects both book buyers and booksellers.”⁶³ Some courts have analogized the First and Second Amendments.⁶⁴ Kopel found that in other contexts, “businesses that provide constitutionally related services have standing in their own right to challenge statutes that injure them.”⁶⁵ To use the language of *Ezell*, many constitutional rights have a “corresponding right” to engage in that right.

In *Pierce v. Society of Sisters*, religious schools successfully raised an individual liberty due process claim on behalf of students and

59. *Id.* at 704.

60. *Ill. Ass’n of Firearms Retailers v. City of Chicago*, 961 F. Supp. 2d 928, 930 (N.D. Ill. Jan. 6, 2014).

61. *Id.* at 930–31.

62. *Id.* at 939.

63. Kopel, *supra* note 45; *see also* Kopel, *supra* note 50.

64. *See, e.g., Ezell*, 651 F.3d at 703 (“Borrowing from the Court’s First Amendment doctrine, the rigor of this judicial review will depend on how close the law comes to the core of the Second Amendment right and the severity of the law’s burden on the right.”).

65. Kopel, *supra* note 45 (collecting cases).

families.⁶⁶ At issue in *Pierce* was both the individual right of children to learn,⁶⁷ and the *corresponding right* of schools to teach the students.⁶⁸ The latter is a necessary incident of the former. Without a guarantee of the freedom to teach, the right to learn would be quite hollow.⁶⁹ In *Craig v. Boren*, the owner of the Honk-N-Holler Grocery store had standing to raise an equal protection claim on behalf of under-age male purchasers.⁷⁰ It was not asserted that the grocer had a constitutional right to sell beer to males under the age of 21.⁷¹ Instead, in order for an underage male to engage in that commercial transaction—based on an unconstitutional classification—a grocer had to be able to provide the beer.⁷² Here the guarantee of the ability to sell the beer was necessary to vindicate the right to buy it.

66. *Pierce v. Soc'y of the Sisters of the Holy Names of Jesus & Mary*, 268 U.S. 510 (1925).

67. *See id.* at 535 (“The fundamental theory of liberty upon which all governments in this Union repose excludes any general power of the State to standardize its children by forcing them to accept instruction from public teachers only. The child is not the mere creature of the State; those who nurture him and direct his destiny have the right, coupled with the high duty, to recognize and prepare him for additional obligations.”).

68. *See id.* (“Appellees are corporations, and therefore, it is said, they cannot claim for themselves the liberty which the Fourteenth Amendment guarantees. Accepted in the proper sense, this is true.. But they have business and property for which they claim protection. These are threatened with destruction through the unwarranted compulsion which appellants are exercising over present and prospective patrons of their schools. And this court has gone very far to protect against loss threatened by such action.” (citation omitted)).

69. *See also* Holder v. Humanitarian Law Project, 561 U.S. 1, 41 (2010) (Breyer, J., dissenting) (“I cannot agree with the Court’s conclusion that the Constitution permits the Government to prosecute the plaintiffs criminally for engaging in coordinated *teaching* and advocacy furthering the designated organizations’ lawful political objectives.” (emphasis added)).

70. *See* *Craig v. Boren*, 429 U.S. 190, 195 (1976) (“As a vendor with standing to challenge the lawfulness of §§ 241 and 245, appellant Whitener is entitled to assert those concomitant rights of third parties that would be ‘diluted or adversely affected’ should her constitutional challenge fail and the statutes remain in force.” (citations omitted)).

71. *See id.* at 192 (“The complaint sought declaratory and injunctive relief against enforcement of the gender-based differential on the ground that it constituted invidious discrimination against males 18-20 years of age.”).

72. *See id.* at 194 (“The legal duties created by the statutory sections under challenge are addressed directly to vendors such as appellant. She is obliged either to heed the statutory discrimination, thereby incurring a direct economic injury through the constriction of her buyers’ market, or to disobey the statutory command and suffer . . . sanctions and perhaps loss of license.” (internal quotation marks

In *Planned Parenthood v. Danforth*, physicians at Planned Parenthood had standing to challenge abortion regulations.⁷³ It was not asserted that there was a constitutional right to provide abortions, but rather that restricting the ability to provide them infringes on the core constitutional right to terminate a pregnancy.⁷⁴ In this sense an individual right is coupled with a constitutional guarantee of the provider of the right. The right to abortion would be meaningless if doctors were prohibited from providing them. In *American Booksellers Association v. Hudnut*, book sellers had standing to challenge a law that criminalized the sale of “pornography.”⁷⁵ There is no constitutional right to sell books (outside of the liberty of contract), though censorship of “pornography” restricts the First Amendment’s guarantee of free speech of those selling books. In a similar fashion, the Court has construed a freedom of association from the First Amendment rights of freedom of speech, assembly, and other constitutional guarantees.⁷⁶

As a matter of first principles, the primary mechanism that allows people to keep and bear arms is the threshold ability to acquire it from someone else. Acquiring a gun entails two separate rights—the rights of the buyer (protected in *Heller*) and the rights of the seller (implied in *Heller*). A constitutional right to bear arms, without a complementary right to acquire (buy and sell) arms, would be meaningless. If the former is protected, and the latter is banned—the Second Amendment would cease to even be a “parchment barrier.”⁷⁷

None of this analysis is to suggest that the state cannot place reasonable regulations on the commercial sale of firearms. Asserting that certain activities are constitutionally protected only subjects them to the same scrutiny the courts have applied to other aspects of the Second Amendment. What cannot stand is an outright ban on

omitted)).

73. See *Planned Parenthood of Cent. Mo. v. Danforth*, 428 U.S. 52, 62–63 (1976).

74. See *id.* at 57–58 (outlining the petitioners’ arguments).

75. *American Booksellers v. Hudnut*, 771 F.2d 323, 327 (7th Cir. 1985), *aff’d mem.*, 475 U.S. 1001 (1986).

76. See *Nat’l Ass’n for Advancement of Colored People v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 460 (1958) (“Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly.”).

77. See generally THE FEDERALIST NO. 48 (James Madison).

the sale or purchase of firearms. Many “longstanding prohibitions” “imposing conditions and qualifications on the commercial sale of arms” would likely satisfy even heightened scrutiny.⁷⁸ However, the same cannot be said of the corresponding right to *make* arms, especially for personal use.

B. *The Right to Make Arms*

Supporting the right to keep and bear arms, and the “corresponding right” to *acquire* arms, is the right to *make* arms. The right to acquire arms must entail, at the minimum, the creation of arms somewhere in the supply chain. The base of the Second Amendment pyramid, before selling, or bearing, must be the creation of guns. If the government permitted the owning of firearms, and the acquisition of firearms, but prohibited the manufacturing or importation of firearms, the vitality of the Second Amendment would implode fairly quickly.

In light of *Heller*, a personal right to make one’s own arms for individual use has a much stronger constitutional pedigree than the right to buy and sell arms from others, especially in the commercial context. There are no “longstanding prohibitions” on making a gun for oneself. Americans have been making their own guns since the founding of the Republic.⁷⁹ This practice, deeply rooted in our nation’s history and tradition, is fairly well-established.⁸⁰ Today, it is legal to make a gun for personal use, with very limited exceptions.⁸¹ In contrast, the sale of firearms has been burdened much more heavily than the right to make firearms.

The right to make arms can be viewed as constitutional guarantee to provide the means necessary to keep and bear arms. The creation of guns, by 3D printing, or other means, directly serves the right protected in *Heller*. A ban on 3D printing would be

78. For a discussion of the Second Amendment and constitutional scrutiny, see Josh Blackman, *The Constitutionality of Social Cost*, 34 HARV. J.L. & PUB. POL’Y 1 (2011).

79. Robert Beckhusen, *Gun Lobby Loves 3D-Printed Weapons*, WIRED (Aug. 10, 2012, 6:30 AM), <http://www.wired.com/2012/08/3d-weapons/> (“As Dudley Brown, executive vice president of the National Association for Gun Rights remarked, ‘People have been making firearms at home since before America was a country.’”).

80. See *Washington v. Glucksberg*, 521 U.S. 702 (1997) (noting that the Constitution “protects those fundamental rights and liberties which are, objectively, deeply rooted in this Nation’s history and tradition” (citations omitted) (internal quotation marks omitted)).

81. *General Questions*, *supra* note 18.

subjected to the heightened scrutiny applied to the Second Amendment. A showing that a person may obtain the gun by other means (buying a manufactured gun from someone else), without a showing of an important state interest, would not be narrowly-tailored enough to survive review. In fact, the ability to make a personalized gun that is not available on the market for oneself may render the countervailing governmental interest less salient. A ban on manufacturing one's own firearms, not for sale, but for personal consumption would hardly be a "longstanding" prohibition, as defined in the dicta in *Heller*.⁸² Since the time of the American Revolution, gun-owners have created their own firearms and ammunition.⁸³

Further, the right is heightened because people can now customize their weapons to meet specific self-defense needs. Peter Jensen-Haxel derives from *Heller* the principle that people have "a strong interest in deciding the characteristics of the defensive device in which to put faith."⁸⁴ Specifically, "[r]ather than accepting pre-packaged attribute bundles determined by marketability, personal design allows someone to choose without limitation the characteristics he or she believes are best suited to self-defense."⁸⁵ People can pick different feature that are "most reliable" for their needs.⁸⁶ For example, one custom-design a gun that strikes the right balance between a longer barrel (more accurate) and shorter barrel (lighter). 3D printing of guns may even "provide the physically disabled with meaningful access to self-defense."⁸⁷ Customizing a firearm for a person with a disability may in fact be a constitutionally-protected reasonable accommodation. Forcing a person to purchase a pre-fabricated gun on the market that fails to meet a person's need would not be a viable alternative and may fail the narrow tailoring necessary to survive constitutional scrutiny.

82. See *District of Columbia v. Heller*, 554 U.S. 570, 626–27 (2008) ("[N]othing in our opinion should be taken to cast doubt on longstanding prohibitions on the possession of firearms by felons and the mentally ill, or laws forbidding the carrying of firearms in sensitive places such as schools and government buildings, or laws imposing conditions and qualifications on the commercial sale of arms.").

83. See Beckhusen, *supra* note 79.

84. Peter Jensen-Haxel, *3d Printers, Obsolete Firearm Supply Controls, and the Right to Build Self-Defense Weapons Under Heller*, 42 GOLDEN GATE U. L. REV. 447, 480–81 (2012).

85. *Id.* at 480.

86. *Id.*

87. *Id.* at 470.

Still, easily obtaining firearms through 3D printing could diminish the efficacy of “presumptively lawful regulatory measures” in place before *Heller*.⁸⁸ If it becomes facile to easily create weapons prohibited by federal law, then the ability to print 3D guns would frustrate federal gun laws. Further, under existing precedent, Congress could still regulate the manufacture of homemade automatic weapons. For example, the Ninth Circuit found that Congress “could prohibit the possession of a homemade machine gun because it could have rationally concluded that the possession of homemade machine guns would substantially affect the interstate market in machine guns.”⁸⁹ The court reaffirmed this holding, finding that *Heller* “has absolutely no impact on *Stewart*’s Commerce Clause holding.”⁹⁰ Even with that caveat, a right to make arms, however defined, is firmly grounded in the Second Amendment.

3D guns will be limited not only by the three guarantee of the Second Amendment, but also by the First Amendment’s guarantee of freedom of speech.

III. THE FIRST AMENDMENT AND 3D-PRINTED GUNS

A. *Information is Speech*

Early advocates of limiting the threat of 3D guns have recognized that once these blueprints are available on the internet, the genie is out of the bottle, and it is too late to stop them. A Department of Homeland Security bulletin stressed that the risk of 3D guns stems from the fact that it is “impossible” to contain the sharing of the blueprints: “Significant advances in [3D] printing capabilities, availability of free digital 3D printer files for firearms components, and difficulty regulating file sharing may present public safety risks.”⁹¹ The bulletin stated the obvious—a ban on 3D-printed guns will not eliminate them—“[p]roposed legislation to ban 3D printing of weapons may deter, but cannot completely prevent their production.”⁹²

88. See *District of Columbia v. Heller*, 554 U.S. 570, 626 n.6 (2008).

89. *Mont. Shooting Sports Ass’n v. Holder*, 727 F.3d 975, 981–82 (9th Cir. 2013) *cert. denied*, 134 S. Ct. 955 (2014) (citing *United States v. Stewart*, 451 F.3d 1071, 1077 (9th Cir. 2006)).

90. *United States v. Henry*, 688 F.3d 637, 638 (9th Cir. 2012).

91. Jana Winter, *Homeland Security Bulletin Warns 3D-Printed Guns May Be “Impossible” to Stop*, FOX NEWS (May 23, 2013), <http://www.foxnews.com/us/2013/05/23/govt-memo-warns-3d-printed-guns-may-be-impossible-to-stop/>.

92. *Id.*

The Department of Homeland Security concluded that “[e]ven if the practice is prohibited by new legislation, online distribution of these digital files will be as difficult to control as any other illegally traded music, movie or software files.”⁹³ In other words, impossible. Therefore, some have proposed stopping 3D guns by cutting off the problem at the source—banning the sharing, and distribution of the 3D CAD files. For example, the State Department has claimed that posting the CAD files for the Liberator on the internet violates export control laws.⁹⁴ One recent article noted that a possible solution would be “to ban the distributions of the designs for 3D printed firearms, and to prosecute people who distribute these designs.”⁹⁵ Such a regime would likely be unconstitutional under the First Amendment.

Electronic communications are considered speech for purposes of the First Amendment.⁹⁶ Even though printing the guns is conduct, at its heart, the government is regulating expression which is “sufficiently imbued with elements of communication to fall within the scope of the First . . . Amendment[.]”⁹⁷ In *Brown v. Entertainment Merchants Association*, the Supreme Court found that “video games qualify for First Amendment protection.”⁹⁸ In the same way that “protected books, plays, and movies that preceded them, video games communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player’s interaction with the virtual world).”⁹⁹ These

93. *Id.*

94. *See infra* Part V.D. for discussion of export control laws.

95. Michael L. Smith, *The Second Amendment Implications of Regulating 3D Printed Firearms* 18–19, available at <http://ssrn.com/abstract=2401563>.

96. *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 851 (1997) (“Taken together, these tools constitute a unique medium—known to its users as ‘cyberspace’—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.”).

97. *Texas v. Johnson*, 491 U.S. 397, 404 (1989) (citation omitted) (internal quotation marks omitted); *see also Holder v. Humanitarian Law Project*, 561 U.S. 1, 27 (2010) (“The Government is wrong that the only thing actually at issue in this litigation is conduct, and therefore wrong to argue that *O’Brien* provides the correct standard of review. *O’Brien* does not provide the applicable standard for reviewing a content-based regulation of speech, and [the material-support statute] regulates speech on the basis of its content. Plaintiffs want to speak to the [groups identified by the government as foreign terrorist organizations] and whether they may do so under [the material-support statute] depends on what they say.” (citations omitted)).

98. *Brown v. Entm’t Merchants Ass’n*, 131 S. Ct. 2729, 2733 (2011).

99. *Id.*

attributes “suffice[] to confer First Amendment protection.”¹⁰⁰ The Supreme Court stressed “whatever the challenges of applying the Constitution to ever-advancing technology, ‘the basic principles of freedom of speech and the press, like the First Amendment’s command, do not vary’ when a new and different medium for communication appears.”¹⁰¹

The Supreme Court has found that a broad species of electronic communications, broadly dubbed “information,” was “speech within the meaning of the First Amendment.”¹⁰² In addition, recent case law¹⁰³ and scholarship¹⁰⁴ have found that data—the output from algorithms—such as search engine results, are speech. In *Brown*, Justice Scalia (inadvertently) made the case for heightened scrutiny for the CAD files of 3D guns. In finding that California’s regulation of violent video games was unconstitutional, he praised California for “(wisely) declin[ing] to restrict Saturday morning cartoons, the sale of games rated for young children, or the *distribution of pictures of guns*.”¹⁰⁵ Why? Because such laws would be patently

100. *Id.*

101. *Id.* (citing *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495, 503 (1952)).

102. *Sorrell v. IMS Health*, 131 S. Ct. 2653, 2667 (2011) (“Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.”).

103. *Jian Zhang v. Baidu.com Inc.*, 11-CIV-3388, 2014 WL 1282730, at *5 (S.D.N.Y. Mar. 28, 2014) (“When search engines select and arrange others’ materials, and add the all-important ordering that causes some materials to be displayed first and others last, they are engaging in fully protected First Amendment expression — ‘[t]he presentation of an edited compilation of speech generated by other persons.’” (alteration in original) (citation omitted)); see *Langdon v. Google, Inc.*, 474 F. Supp. 2d 622 (D. Del. 2007); *Search King, Inc. v. Google Tech., Inc.*, No. CIV-02-1457-M, 2003 WL 21464568 (W.D. Okla. May 27, 2003).

104. *Zhang*, 2014 WL 1282730, at *2 (“The question of whether search-engine results constitute speech protected by the First Amendment has been the subject of vigorous academic debate.” (citing Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445 (2013); Josh Blackman, *What Happens if Data Is Speech?*, 16 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 25 (2014); James Grimmelman, *Speech Engines*, 98 MINN. L. REV. 868 (2014); Eugene Volokh & Donald M. Falk, *Google, First Amendment Protection for Search Engine Search Results*, 8 J.L. ECON. & POL’Y 883 (2012); Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008); Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495 (2013); Michael J. Ballanco, Comment, *Searching for the First Amendment: An Inquisitive Free Speech Approach to Search Engine Rankings*, 24 GEO. MASON U. C.R. L.J. 89 (2013)).

105. *Brown*, 131 S. Ct. at 2740 (emphasis added).

unconstitutional. Pictures of guns are not that conceptually different from more sophisticated 3D blueprints.

3D CAD files of guns are, in truth, nothing more than information—“pictures of guns” defined in lines of source code, rather than graphic visuals. Anyone trained in the language of CAD can understand how this information expresses the ideas. This information explains the shape, size, and dimensions of various types of objects, and offers instructions of how someone can modify or recreate a similar object for their own personal use. The State Department’s letter to Cody Wilson implicitly acknowledges the expressive nature of the source code and specifically refers to the 3D blueprints of the Liberator as “data” in several places.¹⁰⁶ It ordered Wilson to “treat the above technical *data* as ITAR-controlled,” meaning that “all such *data* should be removed from public access immediately.”¹⁰⁷ Consider the CAD source file example discussed earlier.¹⁰⁸ The source code describes in detail three-dimensional objects that, once printed, are expressive.¹⁰⁹ More sophisticated source code could describe works of art, architectural structures, and even the pages of a book. This code, perhaps more so than other types of code, should warrant First Amendment protection because it describes and expresses information about real-world objects that once created, are protected.¹¹⁰

Regulation on the 3D CAD source files is really a regulation on information, and therefore must satisfy constitutional scrutiny. Because bans on 3D CAD files are based on the content of the source code—in this case the object the information expresses—strict scrutiny applies.¹¹¹ Banning the distribution of information about

106. See Letter from Glenn E. Smith, Chief, Enforcement Div., U.S. Dept. of State, to Cody Wilson, Dir., Def. Distributed (May 8, 2013), *available at* <http://www.documentcloud.org/documents/698728-defense-distributed-ddtc.html#document/p1/a101955>.

107. *Id.*

108. See Benchoff, *supra* note 5.

109. See *id.*

110. See Stephan E. Halpern, *Harmonizing the Convergence of Medium, Expression, and Functionality: A Study of the Speech Interest in Computer Software*, 14 HARV. J.L. & TECH. 139, 148–49 (2000) (“Object code that serves as a medium for photographs, movies, music, and literature should not be considered less expressive simply because the medium is constructed of differentiated voltage states instead of traditional materials such as paper or film.”).

111. See *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 115 (1991) (“A statute is presumptively inconsistent with the First Amendment if it imposes a financial burden on speakers because of the content of

how to exercise a constitutional right constitutes a prior restraint of free speech.¹¹² Even more pressing is the fact that banning the distribution of these CAD files also inhibits the ability of others to learn from them. The First Amendment consists of both a right of “creation and dissemination of information.”¹¹³

B. The Right to Create and Disseminate Information

The Supreme Court has long affirmed that the First Amendment is not a one-sided right. The freedom of speech protects not only the speaker, but also the “public and its right to receive information.”¹¹⁴ In *Red Lion Broadcasting Co. v. Federal Communications Commission*, the Supreme Court recognized that the First Amendment protects “the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences.”¹¹⁵ In *Martin v. City of Struthers*, the Supreme Court invalidated a law that banned door-to-door solicitations to hand out literature.¹¹⁶ The Court found the First Amendment “embraces the right [of the solicitor] to distribute literature” and also “necessarily protects the right [of the public] to receive it.”¹¹⁷ In *Stanley v. Georgia*, the Supreme Court unanimously rejected a ban on the “right to receive information and ideas, regardless of their social worth.”¹¹⁸ In *Time, Inc. v. Hill*, the Supreme Court stressed the importance of access to information of matter of public interest.¹¹⁹ “Exposure of the self to others in varying degrees is a concomitant of

their speech.” (citation omitted)).

112. See, e.g., *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971) (finding that an injunction against distributing literature constituted an impermissible prior restraint).

113. *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011) (citing *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001); *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 481 (1995); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985) (plurality opinion)).

114. See *Bigelow v. Virginia*, 421 U.S. 809, 822 (1975) (“The advertisement . . . did more than simply propose a commercial transaction. It contained factual material of clear ‘public interest.’”); see also Ronald K.L. Collins & David M. Skover, *Commerce & Communication*, 71 TEX. L. REV. 697, 730 (1993) (“The informational function is central to the Court’s approval of commercial expression as a form of protected speech.”).

115. *Red Lion Broad. Co. v. Fed. Comm’n’s Comm’n*, 395 U.S. 367, 390 (1969).

116. *Martin v. City of Struthers*, 319 U.S. 141, 146–49 (1943).

117. *Id.* at 143 (citing *Lovell v. Griffin*, 303 U.S. 444, 452 (1938)).

118. *Stanley v. Georgia*, 394 U.S. 557, 564 (1969).

119. See *Time, Inc. v. Hill*, 385 U.S. 374, 388–89 (1967).

life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and press.”¹²⁰

Lamont v. Postmaster General recognized a First Amendment right to an uncensored access to receive mail.¹²¹ *New York Times v. Sullivan* found that the First Amendment promotes an “uninhibited, robust, and wide-open” public debate.¹²² Among the “penumbras formed by emanations” observed in the total constitutional eclipse of *Griswold v. Connecticut* was the right to distribute and receive information about birth control.¹²³ This principle was expanded in Justice Douglas’s concurrence in *Eisenstadt v. Baird*.¹²⁴

Recent cases have reaffirmed the First Amendment right to access information on the internet, and other electronic mediums. *Reno v. Americans Civil Liberties Union* extended the broad protections of the First Amendment to communications on the internet, addressing both the right to express, and to access information: “In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another.”¹²⁵ In *Sable Communications of California v. Federal Communications Commission*, the Court recognized that a ban on adults receiving indecent speech over a “dial-a-porn” service “far exceeds that which is necessary to limit the access of minors to such messages.”¹²⁶ These principles were most clearly articulated in *Sorrell v. IMS Health*, where the Supreme Court found that “The creation and dissemination of information are speech within the meaning of the First Amendment.”¹²⁷

The First Amendment should be viewed in terms of a constitutional right to create and access information. This dual-faceted approach to the freedom of speech accounts for the two key incidents of any First Amendment inquiry—the individual right to express information and the right of individuals in society to learn and consume that information.

Viewed through this lens, the 3D CAD source files of the Liberator assume a high constitutional order of magnitude. Cody

120. *Id.* at 388.

121. *See Lamont v. Postmaster General of U.S.*, 381 U.S. 301, 305–07 (1965).

122. *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964).

123. *Griswold v. Connecticut*, 381 U.S. 479, 482, 485 (1965).

124. *See Eisenstadt v. Baird*, 405 U.S. 438, 457–58 (Douglas, J., concurring).

125. *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 874 (1997).

126. *Sable Comm’ns of Cal., Inc. v. F.C.C.*, 492 U.S. 115, 131 (1989).

127. *Sorrell v. IMS Health*, 131 S. Ct. 2653, 2667 (2011) (emphasis added).

Wilson created the design for a simple handgun. Wilson's expressions should be protected as the "creation . . . of information."¹²⁸ Posting these files on the internet should be protected as the "dissemination of information."¹²⁹ And, the ability of others to learn of this information by downloading the CAD source files embodies the "right to receive information and ideas, regardless of their social worth."¹³⁰ Each of these three activities touches a constitutional base, bringing home the right to 3D-printed guns. Further, scrutiny is even more heightened because the information to be regulated concerns information about another constitutional right—the Second Amendment.

IV. THE HYBRID FIRST AND SECOND AMENDMENTS

The Supreme Court has found, in several contexts, that the First Amendment often bolsters other constitutional rights. The freedom of the press clause supports the right to public trial by jury. Building on *Richmond Newspapers Inc. v. Virginia*, in which a plurality found a "constitutional right of access to criminal trials,"¹³¹ the Court held in *Globe Newspaper Co. v. Superior Court* that the First Amendment protects a "right of access to criminal trials" because "a major purpose of that Amendment was to protect the free discussion of governmental affairs."¹³² In this way, the First Amendment "ensure[s] that the individual citizen can effectively participate in and contribute to our republican system of self-government."¹³³ Free speech supports this complimentary tenant of our Republic. The First Amendment "ensure[s] that this constitutionally protected 'discussion of governmental affairs' is an informed one."¹³⁴ The Court found that "[t]he First Amendment is thus broad enough to encompass those rights that, while not unambiguously enumerated in the very terms of the Amendment, are nonetheless necessary to the enjoyment of other First Amendment rights."¹³⁵

128. *See id.*

129. *See id.*

130. *See Stanley v. Georgia*, 394 U.S. 557, 564 (1969).

131. *Globe Newspaper Co. v. Superior Court for Norfolk Cnty.*, 457 U.S. 596, 603 (1982) (citing *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 558–81 (1980) (plurality opinion)).

132. *Id.* at 604 (quoting *Mills v. Alabama*, 384 U.S. 214, 218 (1966)).

133. *Id.* (citing *Richmond Newspapers*, 448 U.S. at 587–88 (Brennan, J., concurring); *Thornhill v. Alabama*, 310 U.S. 88, 95 (1940)).

134. *Id.* at 605.

135. *Id.* at 604 (citing *Richmond Newspapers*, 448 U.S. at 579–80 (plurality

In the context of religion clause jurisprudence, the Supreme Court recognized a “hybrid claim” that merges together the power of a free speech claim, coupled with a free exercise claim. In *Employment Division v. Smith*, Justice Scalia identified a “hybrid situation” which involves “not the Free Exercise Clause alone, but the Free Exercise Clause in conjunction with other constitutional protections, such as freedom of speech and of the press.”¹³⁶ In these cases, the Court applied heightened scrutiny, in finding that the “First Amendment bars application of a neutral, generally applicable law to religiously motivated action.”¹³⁷ Justice Scalia added that “it is easy to envision a case in which a challenge on freedom of association grounds would likewise be *reinforced* by Free Exercise Clause concerns.”¹³⁸

For example, in *Roberts v. United States Jaycees*, the Court daisy-chained together several constitutional rights to bolster a freedom of association claim—free speech, free exercise, right to petition: “An individual’s freedom to speak, to worship, and to petition the government for the redress of grievances could not be vigorously protected from interference by the State [if] a correlative freedom to engage in group effort toward those ends were not also guaranteed.”¹³⁹ How does this hybrid right work in practice? For example, “an individual who desires to defend the clergy-

opinion)).

136. *Employment Div., Dep’t of Human Res. of Or. v. Smith*, 494 U.S. 872, 881, 882 (1990).

137. *Id.* at 782–33 (citing *Wisconsin v. Yoder*, 406 U.S. 205 (1972); *Cantwell v. Connecticut*, 310 U.S. 296, 304–07 (1940)).

138. *Id.* at 882 (citing *Roberts v. United States Jaycees*, 468 U.S. 609, 622 (1984)). Not everyone was satisfied with the “hybrid exception.” For example, Justice Souter wrote in *Church of the Lukumi Babalu Aye v. City of Hialeah*:

[T]he distinction *Smith* draws strikes me as ultimately untenable. If a hybrid claim is simply one in which another constitutional right is implicated, then the hybrid exception would probably be so vast as to swallow the *Smith* rule, and, indeed, the hybrid exception would cover the situation exemplified by *Smith* But if a hybrid claim is one in which the litigant would actually obtain an exemption from a formally neutral, generally applicable law under another constitutional provision, then there would have been no reason for the Court in what *Smith* calls the hybrid cases to have mentioned the Free Exercise Clause at all.

Church of the Lukumi Babalu Aye, Inc. v. City of Hialeah, 508 U.S. 520, 567 (1993) (Souter, J., dissenting).

139. *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984).

communicant privilege may receive heightened scrutiny if he or she alleges that a mandatory disclosure statute compels him or her to engage in speech that violates deeply held beliefs and also interferes with the free exercise of religion.”¹⁴⁰ In this way, our constitutional rights work together, in tandem, anchored by the freedom of speech.

I should stress, emphatically, that this approach does not even remotely resemble *Griswold*’s “penumbras formed by emanations” test. The hybrid approach focuses on the actual, textual protections in the Constitution. The facts in *Smith*, did “not present such a hybrid situation, but a free exercise claim unconnected with any communicative activity or parental right.”¹⁴¹ This “hybrid” exception is “aimed at the level of scrutiny to be applied by the court in examining the constitutionality of a law burdening religious activity.”¹⁴² While there is some dispute about the appropriate level of scrutiny, many courts have found that coupling together these rights warrants strict scrutiny.¹⁴³

A similar doctrine could be understood in the context of regulating 3D-printed guns. The First and Second Amendments working in tandem would protect speaking and expressing ideas about how to design guns to fit one’s individual needs for self-defense. To use the language of *Smith*, the Second Amendment claim is “reinforced” by the First Amendment. Further, this is not a case where “an invalid free-exercise claim” is “convert[ed]” into “a valid free-speech claim” by virtue of their coupling.¹⁴⁴ Both the First and Second Amendment claims could stand on their own feet.

Communicating about how to exercise the right to keep and bear arms combines the protections of the Free Speech Clause and the Second Amendment. The right to keep and bear arms includes the

140. Christopher R. Pudelski, *The Constitutional Fate of Mandatory Reporting Statutes and the Clergy-Communicant Privilege in A Post-Smith World*, 98 NW. U. L. REV. 703, 737–38 (2004). The Supreme Court avoided the issue of compelled speech about a matter affecting the free exercise of religion by denying certiorari in *Elane Photography, LLC v. Willock*, 309 P.3d 53 (N.M. 2013), cert. denied, 134 S. Ct. 1787 (2014). See Josh Blackman, *Elane Photography is a Bad Vehicle For Religious Liberty Case*, JOSH BLACKMAN’S BLOG (Mar. 23, 2014), <http://joshblackman.com/blog/2014/03/23/elane-photography-is-a-bad-vehicle-for-religious-liberty-case/>.

141. *Employment Div., Dep’t of Human Res. of Or. v. Smith*, 494 U.S. 872, 882 (1990).

142. William L. Esser IV, *Religious Hybrids in the Lower Courts: Free Exercise Plus or Constitutional Smoke Screen?*, 74 NOTRE DAME L. REV. 211, 213 (1998).

143. See *id.* (collecting cases).

144. *Watchtower Bible & Tract Soc’y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 171 (2002) (Scalia, J., concurring).

right to acquire firearms. Acquiring firearms, either through purchasing them, or making them oneself, is not a solipsistic exercise. Potential buyers or manufacturers must be able to discuss, learn, and share ideas about different guns that may meet different self-defense needs. All of these discussions, by themselves, would be protected speech, unless they are deemed to be an “incitement to imminent lawless action”¹⁴⁵ or one of the other rare forms of unprotected speech. Because these communications are made in pursuance of exercising one’s Second Amendment right, the analysis takes on a higher level of scrutiny. Stated differently, the derivative First Amendment right to speak freely about keeping and bearing arms bolsters the primary Second Amendment right. A law prohibiting posting of CAD source files of a handgun hits the unconstitutional trifecta—the right to create speech, the right to disseminate speech, and the right to make arms.

V. THE REGULATION OF 3D GUNS

In this section, I will offer a preliminary analysis of the constitutionality of various proposals to regulate the printing of 3D guns. First, I will review the constitutionality of a law that prohibits the manufacturing, possession, and sale of a 3D gun. Without a showing that these guns are highly dangerous, or pose a special threat to security, these laws banning the personal manufacturing of, and possession of 3D guns, would likely not survive Second Amendment scrutiny. However, the commercial sale of firearms could be regulated in manners consistent with the current sale of traditional firearms.

Second, I will consider a supply-side approach to regulation—a law that would ban the materials used to make 3D guns, or the even gunpowder itself. Efforts to place a substantial burden in front of the right to keep and bear arms would likely violate the Second Amendment.

Third, I turn to the data-centric approach of regulation of 3D guns that would implicate both the First and Second Amendments acting in hybrid. These laws would prohibit the distribution of, and access to, the CAD source files for a 3D gun. In this way, the laws would implicate the rights of both the creator of the CAD files to speak about a constitutional right, and of the recipient to have access to this information and learn about a constitutional right.

145. *Brandenburg v. Ohio*, 395 U.S. 444, 448–49 (1969).

Initially, regulations aimed at protecting intellectual property may sweep in 3D guns. To prevent the infringement of patents, there may be efforts to block the sharing of CAD files of protected objects. Or, industry leaders may install digital rights management technologies onto printers to block printing patented objects. The best alternative model proposed is the Digital Millennium Patent Act, which would use notice-and-takedown approaches to eliminate infringing material. Although, permitting such a system could expand the Digital Millennium Copyright Act's overbroad censoring of constitutionally protected material.

Finally, the International Traffic in Arms Regulations ("ITAR") prohibits the transfer of certain arms and munitions to foreign nationals. The federal government has claimed in its letter to Cody Wilson that the source code for the 3D guns would fall on the protected munitions list.¹⁴⁶ As a result, it would be illegal to post blueprints for a 3D gun online, and allow others to download it. In its current form, this practice would be overbroad, and violate both the First and Second Amendments.

A. Bans on Manufacturing and Possession of 3D-Printed Guns

Today, there does not seem to be any momentum towards a federal ban on manufacturing or possessing of 3D guns for personal use.¹⁴⁷ The sale of 3D guns, like all other guns, would be regulated by existing federal law. There has, however, been some movement on this front at the local level. A proposed law in California, aimed directly at 3D printing, would criminalize making your own firearm without permission (and a serial number) from the state.¹⁴⁸ The bill requires that "prior to manufacturing or assembling a firearm, a person making or assembling the firearm shall . . . apply to the [California] Department of Justice for a unique serial number or other mark of identification . . ."¹⁴⁹ This law would seem to sweep very broadly to anyone who assembles a firearm, whether or not it

146. See Letter from Glenn E. Smith to Cody Wilson, *supra* note 106.

147. Or for any federal gun control laws, for that matter. See Josh Blackman & Shelby Baird, *The Shooting Cycle*, 46 CONN. L. REV. (forthcoming 2014), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2375010.

148. See Jacob Gershman, *California Considers Plastic-Gun Measure*, WALL ST. J. (Jan. 14, 2014 11:03 AM), <http://blogs.wsj.com/law/2014/01/14/california-considers-plastic-gun-measure/>.

149. S.B. 808, Leg., 2013–14 Reg. Sess. (Cal. 2014), available at http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0801-0850/sb_808_bill_20140121_amended_sen_v_95.pdf.

involves 3D printing.¹⁵⁰ The meaning of “assemble” is not defined.¹⁵¹ It is not clear if “assemble” would include taking a gun apart, perhaps to clean or repair it, and reassembling it.

In November of 2014, Philadelphia passed a ban on 3D-printed guns.¹⁵² The sponsor of the bill was not aware of any actual 3D-printed guns in the City of Brotherly Love.¹⁵³ Her legislative director said, “It’s all pre-emptive. It’s just based upon internet stuff out there.”¹⁵⁴ Speaking of preemption, the Philadelphia ban is almost certainly preempted by Pennsylvania law, which provides that “no county, municipality or township may in any manner regulate the lawful ownership, possession, transfer or transportation of firearms, ammunition or ammunition components when carried or transported for purposes not prohibited by the laws of this Commonwealth.”¹⁵⁵

The primary mechanism under federal law to address the manufacturing, and possession of 3D guns would be the Undetectable Firearms Act (“UFA”).¹⁵⁶ This law makes it illegal to “manufacture, import, sell, ship, deliver, possess, transfer, or receive any firearm” that “is not detectable” by a metal detector.¹⁵⁷ The law requires the metallic equivalent of 3.7 ounces of stainless steel to be installed into all firearms.¹⁵⁸ This law was passed in 1988 following an unfounded panic that the Austrian-made Glock pistol was manufactured out of plastic and could evade metal detectors.¹⁵⁹ The idea of an undetectable gun was forever immortalized in the 1990 action thriller *Die Hard 2*, when John McClaine, played by Bruce Willis, described his (fictional) “Glock 7” pistol: “Luggage? That punk pulled a Glock 7 on me. You know what that is? It’s a porcelain gun made in Germany. It doesn’t show up on your airport X-ray

150. See Josh Blackman, *California Bill Would Make It a Crime to Make Your Own Firearm (Without a 3D Printer)*, JOSH BLACKMAN’S BLOG (Jan. 14, 2014), <http://joshblackman.com/blog/2014/01/14/california-bill-would-make-it-a-crime-to-make-your-own-firearm-without-a-3d-printer/>.

151. See S.B. 808.

152. See Simon Van Zuylen-Wood, *Philly Becomes First City to Ban 3-D Gun Printing*, PHILADELPHIA (Nov. 21, 2013, 3:36 PM), <http://www.phillymag.com/news/2013/11/21/philly-becomes-first-city-ban-3-d-gun-printing/>.

153. See *id.*

154. *Id.*

155. 18 PA. CONS. STAT. § 6120(a) (2014).

156. 18 U.S.C § 922(p) (2012).

157. *Id.*

158. See *id.*

159. Barrett, *supra* note 40.

machines here and it costs more than what you make in a month!”¹⁶⁰ Glock has never been made out of plastic or porcelain.¹⁶¹

The UFA was reauthorized in 1998,¹⁶² 2003,¹⁶³ and was set to expire in December of 2013, shortly after the Liberator and 3D guns entered the national conversation. In calling for the UFA’s reauthorization, Attorney General Holder specifically cited the threat of 3D guns, which he called an “extremely serious problem.”¹⁶⁴ He added, “[t]his is a very worrisome threat to law enforcement and to people who fly every day. We can’t have guns legally in circulation that are not detectable by metal detectors.”¹⁶⁵ The “rapid progress” of a 3D-printed AR-15 “lower” receiver—the part that contains the operating guts of the guns—from only being able to handle a few rounds, to 600 rounds in 2013, “sends shivers up the spine of public officials who want to regulate firearms.”¹⁶⁶

Proposals were introduced in the House¹⁶⁷ and the Senate¹⁶⁸ that would have expanded the reach of the law to criminalize certain types of 3D-printed guns.¹⁶⁹ Specifically, the Undetectable Firearms Modernization Act (“UFMA”) would have extended the UFA ban to “undetectable firearm receivers made by individuals” and “undetectable ammunition magazines by individuals.”¹⁷⁰ While in the past, the manufacturing of firearms for personal consumption was largely unregulated, now do-it-yourself guns would become a federal crime.

It is clear UFMA was proposed in direct response to the Liberator, as it was mentioned numerous times during the legislative debate. The findings for these bills specifically cited the fact that “3D printers . . . are quickly advancing to a point where it will soon be possible to fabricate fully operational firearm

160. *DIE HARD* (20th Century Fox 1988).

161. See generally PAUL M. BARRETT, *GLOCK: THE RISE OF AMERICA’S GUN* (2012).

162. Act of Oct. 21, 1998, Pub. L. No. 105-277, § 649, 112 Stat. 2681, 3209 (1998).

163. Act of Dec. 9, 2003, Pub. L. No. 108-174, § 649, 117 Stat. 2481 (2003).

164. *Holder Takes Aim at 3-D Guns, Calls for Renewal of Metal Detection Law*, *supra* note 34.

165. *Id.*

166. Desai & Magliocca, *supra* note 3 (manuscript at 20).

167. Undetectable Firearms Modernization Act, H.R. 1474, 113th Cong. (2013).

168. Undetectable Firearms Modernization Act, S. 1149, 113th Cong. (2013).

169. Murphy, *supra* note 16.

170. Undetectable Firearms Modernization Act, S. 1149, 113th Cong. §§ 4, 5 (2013); Undetectable Firearms Modernization Act, H.R. 1474, 113th Cong. §§ 4, 5 (2013).

components.”¹⁷¹ Senator Chuck Schumer was concerned that 3D printing can “make what was once a hypothetical threat into a terrifying reality. We are actively exploring all options to pass legislation that will eliminate the threat of completely undetectable weapons.”¹⁷² Ultimately, these modifications to the law were defeated. The UFA was reauthorized without amendments on December 9, 2013¹⁷³ and signed into law by President Obama’s autopen.¹⁷⁴

A requirement that a firearm contain some small amount of metal will likely survive any constitutional scrutiny. The UFA allows 3D guns to be printed from plastic so long as there is a small piece of metal installed into it.¹⁷⁵ This approach is narrowly tailored to make it easier to detect firearms in certain “sensitive places” guarded by metal detectors, or body scanners (which could detect an entirely plastic gun).¹⁷⁶ Adding a small amount of metal would not alter the operation, effectiveness, or usability of the firearm, so the burden seems *de minimis*.

Though, it is doubtful how effective this law would be. Even if the UFMA were passed, it could easily be evaded by adding a small amount of metal, such as a roofing nail, which can be used as a firing pin for the gun. In fact, the plans for the Liberator called for the installation of a piece of metal (the firing pin made out of a nail) that would satisfy the UFA.¹⁷⁷ Someone intent on inflicting harm could just as easily remove the nail to evade security. So-called “ghost-guns,” made out of plastic parts,¹⁷⁸ have been in existence long before 3D printing was in existence.

171. Undetectable Firearms Modernization Act, S. 1149, 113th Cong. § 2 (2013); Undetectable Firearms Modernization Act, H.R. 1474, 113th Cong. § 2 (2013).

172. Barrett, *supra* note 35.

173. Act of Dec. 9, 2003, Pub. L. No. 108-174, § 649, 117 Stat. 2481 (2003).

174. See Josh Blackman, *Undetectable Gun Act, Autopen, and Pocket Veto*, JOSH BLACKMAN’S BLOG (Dec. 10, 2013), <http://joshblackman.com/blog/2013/12/10/undetectable-gun-act-autopen-and-pocket-veto/>.

175. See 18 U.S.C § 922(p) (2012).

176. See *District of Columbia v. Heller*, 554 U.S. 570, 626–27 (2008) (affirming the validity of laws “forbidding the carrying of firearms in sensitive places such as schools and government buildings”).

177. See Sebastian Anthony, *The Liberator: The First Downloadable 3D-Printed Gun Gets Test Fired*, EXTREME TECH (May 6, 2013, 6:23 AM), <http://www.extremetech.com/extreme/155084-the-liberator-the-first-downloadable-3dprinted-gun-gets-test-fired>.

178. See *California Bill Aims to Regulate 3-D “Ghost Guns”*, RT (Jan. 14, 2014 11:55 AM), <http://rt.com/usa/california-bill-ghost-guns-senator-577/>.

B. Bans on Materials Used For Printing 3D Guns

An alternative to banning the manufacturing or possession of 3D guns would be to ban, or heavily regulate, the supplies needed to print a 3D gun. One proposal, noted by Professors Desai and Magliocca, would involve the regulation of the “material used to make the [3D] gun.”¹⁷⁹ This directed approach would restrict access to the “particular blend of plastic or metal can be shaped into reliable guns.”¹⁸⁰ If these guns can be manufactured from a “common material”—more likely—“then the answer would be to alert law enforcement authorities when someone buys an unusually large amount of that input, much as some states do with fertilizer because terrorists can make bombs out of that.”¹⁸¹

There are practical and constitutional problems with this approach. Practically, it would be virtually impossible to single out the type of plastic used to make 3D guns, as there many, many different materials that can be used. In fact, 3D guns are not limited to plastic parts. Solid Concepts has built a 3D-printed metal gun.¹⁸² Rather than using plastic powder, the 3D printer relies on finely-grounded metal powder to create three-dimensional parts.¹⁸³ Constitutionally, banning a certain type of plastic that can be used for 3D printing would unduly regulate vast amounts of innovative non-gun designs people can create. This would burden many protected forms of expression. The state’s interest in banning a certain type of plastic, because it may be used in a gun design, along with thousands of other designs, would be overbroad.

Professors Desai and Magliocca further suggested that it may be necessary to limit access to “bullets” and “gunpowder.”¹⁸⁴ A professor at Cornell University noted that, “[p]erhaps the only way forward, if we choose to try and control this, is to control the gunpowder—the explosives—and not the actual device.”¹⁸⁵ Limiting access to

179. Desai & Magliocca, *supra* note 3 (manuscript at 21).

180. *Id.*

181. *Id.*; see also Jensen-Haxel, *supra* note 84, at 469 (“The most obvious legislative response would be to criminalize the act of making or possessing homemade guns. More narrowly, new rules might ban firearms made by specific processes (e.g., additive manufacturing) or made from certain materials employed by those processes (e.g., plastics and powder-based metals).”).

182. Blackman, *supra* note 31.

183. See *id.*

184. Desai & Magliocca, *supra* note 3 (manuscript at 21).

185. See Robert Beckhusen, *3-D Printing Pioneer Wants Government to Restrict Gunpowder, Not Printable Guns*, WIRED (Feb. 19, 2013 6:30 AM), <http://www.wired>

ammunition, and the gunpowder needed to load ammunition, would have serious constitutional problems.

The Supreme Court has held that denying someone the equipment to exercise a right is itself a constitutional violation. For example, the Supreme Court found that a Minnesota law that imposed a tax on newspaper ink and paper “violates the First Amendment” because it “singles out the press.”¹⁸⁶ Under such a regime, people were free to own newspapers, and could freely buy and sell newspapers, but the means necessary to create the newspapers was unconstitutionally burdened. Banning gunpowder and bullets is comparable to banning newspaper ink and paper. As Professor Nicholas Johnson explained, “Even though *Heller* did not explicitly address ammunition, it would eviscerate the right to say that guns are protected but ammunition is not.”¹⁸⁷ Neither of these proposals are constitutionally viable, to say nothing of the public backlash against informing the 100 million Americans who own firearms that they are restricted in their purchase bullets or gunpowder due to a weak concern of 3D-printed guns.¹⁸⁸

C. Intellectual Property Regulations and 3D-Printed Guns

Although the promise of 3D printing is great, the ability to instantly and easily reproduce objects that may be protected by patents, trademarks, copyrights, or trade dresses, will create a quantum shift in intellectual property law. Professors Desai and Magliocca have observed that this technology is “launching an Industrial Counter-Revolution, and the laws governing the way things are made will need to make peace with the reality of digitized objects made of simple raw materials and software.”¹⁸⁹ The “rapid

.com/dangerroom/2013/02/gunpowder-regulation/ (emphasis added).

186. *Minneapolis Star & Tribune Co. v. Minnesota Comm’r of Revenue*, 460 U.S. 575, 591 (1983).

187. Nicholas J. Johnson, *Administering the Second Amendment: Law, Politics, and Taxonomy*, 50 SANTA CLARA L. REV. 1263, 1265 (2010) (“Even though *Heller* did not explicitly address ammunition, it would eviscerate the right to say that guns are protected but ammunition is not.”).

188. See PEW RESEARCH CTR., PERSPECTIVES OF GUN OWNERS, NON-OWNERS: WHY OWN A GUN? PROTECTION IS NOW TOP REASON 16, available at <http://www.people-press.org/files/legacy-pdf/03-12-13%20Gun%20Ownership%20Release.pdf> (detailing survey finding that 24% of adult Americans own guns). For a discussion on public perceptions of the right to keep and bear arms, see Blackman & Baird, *supra* note 147.

189. Desai & Magliocca, *supra* note 3 (manuscript at 3) (footnote omitted).

uptake at different layers of society [of 3D printing] indicates disruption of some sort is at hand and growing.”¹⁹⁰ 3D printing challenges the basic assumption underlying patent law—that “the cost to infringe is relatively high.”¹⁹¹ The manufacturing sector is very concerned about 3D printing, as it gives people the ability to create items at home, vitiating the need for manufacturing services.¹⁹²

The proliferation of 3D printing will “reduce the value of many patents, some copyrights, and all trade dress, because even the best efforts to stop this surge in infringement will fall short.”¹⁹³ Yet, one of the greatest benefits of 3D printing is that it will “accelerate the pace at which design, prototyping, and entrepreneurial launches and failures occur,” leading to “rapid, unpredictable experimentation, faster learning, and increased knowledge growth.”¹⁹⁴

An alternate approach to regulating 3D guns could be built on an intellectual property regime aimed at prohibiting the printing of patented objects. I consider two possible approaches to an intellectual-property approach to regulating 3D printing, and 3D-printed guns in particular. First, government-mandated filters can be installed throughout the internet to stop the sharing of certain prohibited files, such as CAD files. If the files being blocked pertain to constitutionally protected information, this would amount to an unconstitutional prior restraint of protected speech. Second, I look at laws requiring the installation of Digital Rights Management technology in 3D printers that would not permit printing certain prohibited files. This raises the specter of chilling wide swaths of protected expressions. Finally, I consider a vastly-superior alternative, the Digital Millennium Patent Act (“DMPA”), based on the Digital Millennium Copyright Act’s (“DMCA”) notice-and-takedown process, as described by Professors Desai and Magliocca. This system would allow for the takedown of files that infringe on patents but would permit sharing of other constitutionally protected materials.

190. *Id.*

191. *Id.*

192. See John Biggs, *Home 3D Printing Is Killing the Manufacturing Industry*, TECHCRUNCH (Oct. 2, 2012), <http://techcrunch.com/2012/10/02/home-3d-printing-is-killing-the-manufacturing-industry/>.

193. Desai & Magliocca, *supra* note 3 (manuscript at 5).

194. *Id.* (manuscript at 6).

1. Filtering CAD Files on the internet

Today, mechanisms exist to detect, and filter files shared on the internet that violate certain copyrights. For example, the popular video-sharing site YouTube has installed a Content ID system. As Professors Desai and Magliocca have noted:

Copyright holders share digital fingerprints of their work with YouTube. When a user creates a file, it is compared against the fingerprint database. If it appears to be a match, the copyright holder is notified and then chooses how to proceed by either issuing a takedown notice under the DMCA, doing nothing, or choosing to place advertisements and/or links to buy the song on the page where the video is watched.¹⁹⁵

Dropbox, a file-sharing system, uses a similar process to determine if users are sharing pirated files—they rely on a “technique known as ‘file hashing against a blacklist’ to block pre-selected files from being shared person-to-person over its servers.”¹⁹⁶ This “hashing—a simple algorithmic tool which maps data of arbitrary length to data of a fixed length—to produce a unique identifier for every file you upload (it also then encrypts your file so others can’t read them).”¹⁹⁷

These filters are not limited to individual sites. The Copyright Alerts System (“CAS”) is an internet-wide filter that can identify illegally shared files being downloaded.¹⁹⁸ CAS was created through an agreement among the five largest Internet Service Providers (AT&T, Cablevision, Comcast, Time Warner, or Verizon) and media companies.¹⁹⁹ By closely monitoring peer-to-peer filing share sites, CAS can inspect what a user is downloading, and match its signature (called a “hash”) against a set of signatures for known pirated files.²⁰⁰ If the system determines an illegal file is being downloaded, it offers a “graduated response,” ranging from an email

195. *Id.* (manuscript at 53 n.132).

196. Jamie Condliffe, *How Dropbox Knows When You’re Sharing Copyrighted Files*, GIZMODO (Mar. 31, 2014 8:56 AM), <http://gizmodo.com/how-dropbox-knows-when-youre-sharing-copyrighted-files-1555180683>.

197. *Id.*

198. Kevin Collier, *Your Guide to Life Under the Copyright Alerts System*, DAILY DOT (Feb. 20, 2013), <http://www.dailydot.com/news/copyright-alerts-system-six-strikes-primer-guide/>.

199. *See id.*

200. *See id.*

notification to throttling maximum internet speeds to a slow crawl to termination of the account.²⁰¹

Even if this system is implemented voluntarily by private parties, and not by government mandate, the “service providers are acting ‘in the shadow of the law,’ motivated by the state action that established copyright liability and the DMCA.²⁰² Government cannot insulate itself from responsibility for this abridgment of free speech by routing its influence through third-party service providers.”²⁰³

A similar provision, whether mandated by the government, or implemented voluntarily could be used to police downloading 3D blueprints for guns. Any uploads of a banned blueprint that has signatures of being a 3D gun, could be flagged, and filtered. Anyone who attempts to download the file could be reported to the authorities. Already, popular 3D printing file-sharing sites have removed all 3D guns. Thingiverse, a database of downloadable 3D files, has banned 3D gun blueprints.²⁰⁴ Somewhat ironically, Kim Dotcom, the world’s most famous intellectual pirate, deleted all links to the blueprint of the Liberator from his file-sharing website.²⁰⁵ In response, Wilson created DEFCAD, which he dubbed “the island of misfit objects.”²⁰⁶

The folly of censoring the blueprints is that the simplest encryption can evade filtering. The “Disarming Corruptor” algorithm allows designers to encrypt the appearance of blueprints using a special key, so that the CAD file does not resemble a gun, and only those with the key can unscramble the designs.²⁰⁷ Further,

201. *Id.*

202. Wendy Seltzer, *Free Speech Unmoored in Copyright’s Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 190 (2010) (citing Robert H. Mnookin & Lewis Kornhauser, *Bargaining in the Shadow of the Law: The Case of Divorce*, 88 YALE L.J. 950 (1979)).

203. *Id.*

204. See Andy Greenberg, *3D-Printing Firm Makerbot Cracks Down on Printable Gun Designs*, FORBES (Dec. 19, 2012 4:30 PM), <http://www.forbes.com/sites/andygreenberg/2012/12/19/3d-printing-startup-makerbot-cracks-down-on-printable-gun-designs/>.

205. See Gregory Ferenstein, *Offshore 3D Printed Gun Blueprint Protector Kim Dotcom Reportedly Deleting Files*, TECHCRUNCH (May 11, 2013), <http://techcrunch.com/2013/05/11/offshore-3d-printed-gun-blueprint-protector-kim-dotcom-reportedly-deleting-files/>.

206. See Brian Benchoff, *DEFCAD, The Island of Misfit Objects*, HACKADAY (Mar. 12, 2013), <http://hackaday.com/2013/03/12/defcad-the-island-of-misfit-objects/>.

207. See Georgi Kantchev, *Authorities Worry 3-D Printers May Undermine Europe’s Gun Laws*, N.Y. TIMES (Oct. 17, 2013), <http://www.nytimes.com/2013/10/18/business/international/european-authorities-wary-of-3-d-guns-made-on-printers>.

2014]

3D PRINTED GUNS

517

information cannot be controlled. DEF CAD, if shut down, will spawn countless other mirror sites that can replicate the files.²⁰⁸ Filtering will not work, and will only serve to over-broadly sweep in constitutionally protected expressions.

2. Digital Rights Management on 3D Printers

Digital Rights Management (“DRM”) is a set of controls installed on computers and accessories to prevent the reproduction of certain protected materials.²⁰⁹ For example, eBooks you purchase on the Amazon Kindle store cannot be copied onto other devices without permission due to DRM.²¹⁰ Many CDs and DVDs cannot be duplicated due to DRM installed on the disks.²¹¹ Specifically, because the song and movie are copyrighted, they were encoded with a certain digital signature. A DRM-equipped device, such as an iPad or Kindle, will read that signature, and prevent their reproduction.

Similar technologies could be installed onto 3D printers. One startup that distributes 3D printers opposed government intervention, favored “industry self-imposed regulation, perhaps using DRM-style access control technologies.”²¹² If a CAD file would create an object that is protected by a patent or a trade dress, DRM technology could be implemented to prevent it from being printed. A

html.

208. See Tim Murphy, *State Department Forces Texas Law Student to Take Down Instructions for 3-D-Printed Guns*, MOTHER JONES (May 9, 2013, 4:38 PM), <http://www.motherjones.com/mojo/2013/05/state-department-cody-wilson-defense-distributed> (“As with everything else on the Internet, the takedown notice from the DTCC has its limitations. For one thing, there are already a number of ‘mirror’ sites that essentially replicate DEF CAD but are not controlled by Wilson—or anyone in the United States, for that matter. You can also download the plans for the Liberator or various component parts from the Pirate Bay, the notorious Swedish file-sharing index site.”).

209. See generally Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537 (2005).

210. See Cyrus Farivar, *DRM Be Damned: How to Protect Your Amazon E-Books from Being Deleted*, ARSTECHNICA (Oct. 25, 2012, 8:15 PM), <http://arstechnica.com/gadgets/2012/10/drm-be-damned-how-to-protect-your-amazon-e-books-from-being-deleted/>.

211. See Julia Layton, *How Digital Rights Management Works*, HOWSTUFFWORKS, <http://computer.howstuffworks.com/drm4.htm> (last visited Jun. 14, 2014).

212. Lorenzo Franceschi-Biccherai, *3D-Printed Weapons Builder Says He’s Ready to Print Entire Handgun*, MASHABLE (Apr. 24, 2013), <http://mashable.com/2013/04/24/3d-printed-handgun/>.

patent has already been granted that would install a DRM filter into a 3D printer.²¹³ Such printers would refuse to print something that a user does not have permission to print.²¹⁴ With this DRM, “[e]ven if users were able to obtain digital blueprints to print firearms, they would not be able to print from these blueprints.”²¹⁵ Relatedly, Stratasys, a maker of 3D printers, repossessed Cody Wilson’s printer,²¹⁶ explaining that they would not permit him to build a gun with it.²¹⁷

It is not inconceivable for the private industry groups, or even the government, to mandate that 3D printers will not print certain blueprints that have a certain DRM signature on them. In other words, if you tried to print a 3D gun, the 3D printer would not work. An analogy to this would be the SSL (secure socket layer) certificates used on certain commercial web sites. In order to engage in secure online transactions, a site must have a certain public and private key. If they do not match, the transaction would not work. Congress could require that 3D printers only print if a certain key is provided.

The danger of a digital rights management scheme is that the “could fall into path-dependent solutions where creators are told to use a 3D printer only for certain purposes.”²¹⁸ As Professors Desai and Magliocca note, “[i]ncumbent patentees may lobby Congress to pass statutes that hobble the 3D printing industry.”²¹⁹ “Incumbents will challenge the technology,” and “demand that the law limit” 3D printing.²²⁰ Specifically, these “efforts could use the fear of guns as a

213. U.S. Patent No. 8,286,236 (filed Jan 31, 2008) (granted on October 9, 2012 to Intellectual Ventures of Bellevue, Washington for a system lending a 3D printer the ability to assess whether a computer design file it is reading has an authorization code that grants access for printing—and preventing the machine from printing if it does not—whether it is a solid object, a textile, or even a food that is being printed)

214. See Paul Marks, *New Patent Could Saddle 3D Printers with DRM*, GIZMODO (Oct. 18, 2012 4:52 AM), <http://gizmodo.com/5952780/new-patent-could-saddle-3d-printers-with-drm>.

215. Smith, *supra* note 95, at 19.

216. See *Imagine if Your Biggest Part in the Human Drama Was to Stand in the Way of an Innovation*, WIKIWEP DEVBLOG (2012), <http://defdist.tumblr.com/post/32381907035/imagine-if-your-biggest-part-in-the-human-drama>.

217. See Paul Marks, *DIY Gun Project Misfires as 3D Printer Is Seized*, NEW SCIENTIST (Oct. 2, 2012 10:31 AM), <http://www.newscientist.com/article/dn22323-diy-gun-project-misfires-as-3d-printer-is-seized.html>.

218. Desai & Magliocca, *supra* note 3 (manuscript at 56).

219. *Id.* (manuscript at 20–21).

220. *Id.* (manuscript at 7).

rallying cry for limits on 3D printing that stretch beyond what may be required for those limited issues.”²²¹

The primary difficulty with using an intellectual property regime to police 3D guns is that the opposition to 3D guns is not based on intellectual property. No one claims that the Liberator violates any patents. In fact the Liberator was created as an open-sourced document.²²² And this was a firearm model that was in the public domain for decades, available to anyone.²²³ Yet, the infrastructures that could police infringing 3D CAD files could easily be extended to files deemed illicit—such as 3D guns.

In other words, the government could simply hijack the existing process to censor and block prohibited CAD files as a means to eliminate 3D guns. “[C]ompanies with a vested interest in the current system must not be allowed to use concerns about homemade guns or other distractions as an excuse to shackle 3D printing.”²²⁴ There is always the risk of a Baptist and Bootlegger coalition forming.²²⁵ Manufacturers who seek to shut down 3D-printing will ride the wave of opposition to 3D guns to stifle this innovative industry. Desai and Magliocca conclude that “[t]he understandable desire to prevent individuals from making untraceable or illegal guns should not cause undue alarm.”²²⁶

Alas, the seeds have already been planted. The Create it REAL 3D printer has “developed software that looks for the characteristics of weapon designs and, when detected, blocks the printer from

221. *Id.* (manuscript at 21).

222. Wilson claims that the fact that the blueprint is open-sourced exempts it from the scope of export control laws. See Andy Greenberg, *State Department Demands Takedown of 3D-Printable Gun Files for Possible Export Control Violations*, FORBES (May 9, 2013 2:36 PM), <http://www.forbes.com/sites/andygreenberg/2013/05/09/state-department-demands-takedown-of-3d-printable-gun-for-possible-export-control-violation/> (“Defense Distributed is excluded from the ITAR regulations under an exemption for non-profit public domain releases of technical files designed to create a safe harbor for research and other public interest activities. That exemption, he says, would require Defense Distributed’s files to be stored in a library or sold in a bookstore. Wilson argues that Internet access at a library should qualify under ITAR’s statutes, and says that Defcad’s files have also been made available for sale in an Austin, Texas bookstore that he declined to name in order to protect the bookstore’s owner from scrutiny.”).

223. See *id.*

224. Desai & Magliocca, *supra* note 3 (manuscript at 7).

225. See Bruce Yandle, *Bootleggers and Baptists: The Education of a Regulatory Economist*, REGULATION, May–June 1983, at 12.

226. Desai & Magliocca, *supra* note 3 (manuscript at 21).

making a firearm.”²²⁷ Regulating firearms is far beyond the purview of intellectual property law, and it should not be quietly co-opted for this purpose. I agree with Professors Desai and Magliocca that concern about 3D-printed guns is a red herring regarding possible regulation.²²⁸ Congress should avoid the urge of muddying the intellectual property waters by tackling the difficult and constitutionally sensitive area of 3D guns under the guise of protecting patents.²²⁹ “Trying to stop or dictate the way a 3D printer is used unduly limits the potential of these general-purpose machines and mimics the failed DRM ideas of the copyright industry.”²³⁰

3. Digital Millennium Patent Act

Rather than seeking government-mandated filtering of protected objects or installing DRM into printers, in a path-breaking article, Professors Desai and Magliocca propose a “Digital Millennium Patent Act” modeled on the Digital Millennium Copyright Act.²³¹ They offer a two-part legislative strategy to balance these important interests: Congress must “(1) remove[] the shadow of infringement liability from some people who use 3D printers for personal purposes; and (2) provide[] clear rules for websites that host the programs that let these devices function.”²³² Specifically, Congress should create “infringement exemption for personal 3D printing . . . that would not facilitate large-scale commercial manufacturing,” and a “Digital Millennium Patent and Trademark Act (DMPA) . . . that would impose notice and takedown rules on the sites that host 3D printing software.” Under such a regime, “website that serves as a conduit for 3D printer software should be liable for contributory infringement if it refuses to take down a file after receiving a plausible complaint from a patentee.”²³³

227. Georgi Kantchev, *Authorities Worry 3-D Printers May Undermine Europe’s Gun Laws*, N.Y. TIMES (Oct. 17, 2013), <http://www.nytimes.com/2013/10/18/business/international/european-authorities-wary-of-3-d-guns-made-on-printers.html>.

228. See Desai & Magliocca, *supra* note 3 (manuscript at 17–23).

229. See *id.* (manuscript at 12) (“Lower costs, the ability to make specialized and just-in-time parts, and a return to local manufacturing are all positive developments that should be embraced. Yet these advances will threaten if not destroy many firms and jobs that live off rents from intellectual property.”).

230. *Id.* (manuscript at 56).

231. See *id.* (manuscript at 7).

232. *Id.*

233. *Id.* (manuscript at 44).

This approach would build on the Digital Millennium Copyright Act's "notice-and-takedown rules" which most "sites are already complying with . . . for files involving copyrights."²³⁴ Creators of protected work could request that an internet site remove any CAD file. If the internet site reasonably complies, it would not be liable for infringement. The person who posted the file would have some recourse to challenge the takedown. Extending this regime to protect patents would avoid the "odd" regime of having "two sets of rules for these clearinghouses, one for copyrights and another for patents and trade dress."²³⁵

A Digital Millennium Patent and Trademark Act would serve as a powerful tool to protect intellectual property. Already, several 3D printing repositories "such as Thingiverse and Shapeways, have a notice-and-takedown policy, in part because some of their CAD files cover copyrighted content."²³⁶ One of the greatest benefits of the DMPA is that it would not require filtering of protected 3D CAD files, or prohibiting the printing of these files on printers. To the extent that Congress considers an approach to regulate the intellectual property implications of 3D printing—of which there are many—the DMPA would be a viable option to pursue.

Though, in some cases, it may lead to an undue chilling of speech, in much the same way the DMCA does. If a similar "takedown procedure took place through the courts, it would trigger First Amendment scrutiny as a prior restraint—silencing speech before an adjudication of unlawfulness."²³⁷ How can it be that in the "wake of *Citizens United*," "copyright law [can] remove political videos from public reach when campaign finance law [can] not?"²³⁸

While this analysis should in no way be viewed as an attack or criticism of regimes aimed at protecting intellectual property, care must be taken to ensure that these regulations are not expanded beyond the purpose of protecting intellectual property. Regulations to protect intellectual property have been upheld against free speech challenges by the Supreme Court, as noted in *Eldred v. Ashcroft*: "[W]hen . . . Congress has not altered the traditional contours of copyright protection, further First Amendment scrutiny is unnecessary."²³⁹ The authors acknowledge this point, noting that "[a]lthough the framework created by the DMCA is still

234. *Id.* (manuscript at 53).

235. *Id.*

236. *Id.* (manuscript at 52).

237. Seltzer, *supra* note 202, at 176.

238. *Id.*

239. *Eldred v. Ashcroft*, 537 U.S. 186, 215, 221 (2003).

controversial in some quarters, the notice-and-takedown system works reasonably well.”²⁴⁰ But, notwithstanding *Eldred*, the use of notice-and-takedown systems for non-patented expressions that are constitutionally protected would run headlong into the First and Second Amendments.

D. Export Controls of Information about 3D Guns

Beyond regulating the manufacturing and possession of 3D guns, and the materials needed to create them, the most constitutionally troubling regulatory regime would prohibit the exchange of the 3D CAD blueprints. Even the Undetectable Firearms Modernization Act would not have restricted “what kind of [3D] printer files you can post online.”²⁴¹ As Rep. Steve Israel, who co-sponsored the Undetectable Firearms Modernization Act said, “Nobody is regulating 3D printers in this bill. Nobody is regulating the ability of people to acquire digital blueprints in this bill.”²⁴² But other provisions of federal law could do just that. Shortly after Cody Wilson published the CAD source code for the Liberator, the State Department sent him a letter *strongly hinting* that posting this information online violated export control laws that were meant to prohibit sharing weapon technology with foreign nationals.²⁴³ This prior restraint of speech about the right to keep and bear arms conflicts with the First and Second Amendments.

1. ITAR and the First Amendment

Under the Arms Export Control Act of 1976 (“AECA”),²⁴⁴ the United States government operates two overlapping systems to limit what can be exported.²⁴⁵ The first regime is the Department of Commerce’s Commerce Control List (“CCL”),²⁴⁶ which controls “dual-

240. Desai & Magliocca, *supra* note 3 (manuscript at 53).

241. See Murphy, *supra* note 16.

242. Lorenzo Franceschi-Biccherai, *Law Banning 3D-Printed Guns Up for Crucial Vote*, MASHABLE (Dec. 2, 2013), <http://mashable.com/2013/12/02/3d-printed-guns-law-renew/>.

243. See Letter from Glenn E. Smith to Cody Wilson, *supra* note 106.

244. 22 U.S.C. § 2778 (2012).

245. See David R. Fitzgerald, *Leaving the Back Door Open: How Export Control Reform’s Deregulation May Harm America’s Security*, 15 N.C.J.L. & TECH. ON. 65 (2014).

246. *Commerce Control List*, U.S. DEPT. OF COM., <http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl> (last visited May 31, 2013).

use items, i.e., commercial items with possible military applications, and some military items of lesser sensitivity.”²⁴⁷

The second regime is the United States Munitions List (“USMIL”),²⁴⁸ operated by the Department of State pursuant to the International Traffic in Arms Regulations (“ITAR”).²⁴⁹ ITAR restricts the export of so-called Significance Military Equipment (“SME”), defined as “articles for which special export controls are warranted because of their capacity for substantial military utility or capability.”²⁵⁰ Prior authorization from the State Department is required prior to exporting any SME listed on ITAR.²⁵¹ The USMIL lists 21 categories of technologies, including most relevant for our purposes, many types of firearms and “munitions.”²⁵²

Salient to this discussion, there have been several attempts by the federal government to use ITAR as a prohibition on sharing the source code for encryption algorithms outside the United States. Encryption refers to “the process of converting a message from its original form (‘plaintext’) into a scrambled form (‘ciphertext’).”²⁵³ When performed on a computer, encryption relies on an “algorithm, a mathematical transformation from plaintext to ciphertext, and a key that acts as a password.”²⁵⁴ Encryption software is programmed primarily through “source code,” which represents instructions to “the computer’s circuitry to execute the encoding process.”²⁵⁵ The encryption source code, much like the CAD source code described earlier, “can [be] read and underst[ood] by “[i]ndividuals familiar with a particular computer programming language.”²⁵⁶

There are three leading cases that discuss whether a ban on the export of the encryption source code constitutes a prior restraint in violation of the First Amendment. The first case, *Karn v. United States Department of State*, upheld such a ban.²⁵⁷ Even assuming that the source code was protected speech, the countervailing

247. Office of the Press Secretary, *Fact Sheet: Implementation of Export Control Reform*, WHITE HOUSE (Mar. 8, 2013), <http://www.whitehouse.gov/the-press-office/2013/03/08/fact-sheet-implementation-export-control-reform>.

248. 22 C.F.R. § 121.1 (2013).

249. *Id.*

250. *Id.* § 120.7(a).

251. *Id.* § 123.1.

252. *Id.* § 121.1.

253. *Junger v. Daley*, 209 F.3d 481, 482 (6th Cir. 2000).

254. *Id.*

255. *Id.*

256. *Id.*

257. See *Karn v. U.S. Dep’t of State*, 925 F. Supp. 1, 10–13 (D.D.C. 1996).

interests in preserving national security trumped.²⁵⁸ The second case (which was withdrawn following the grant of a petition for rehearing en banc), *Bernstein v. United States Department of Justice*, found that the source code was encrypted speech and that it would be difficult for the government to justify the prior restraint based on national security interests.²⁵⁹ Third, *Junger v. Daley* considered a case where a law professor sought to upload encryption source code to his website to demonstrate the code to his students.²⁶⁰ The Sixth Circuit found that the source code for encryptions algorithms was speech, and that the government bears a strong burden to show that the national security interests justify this prior restraint.²⁶¹ A careful study of each case informs the constitutional inquiry of the First Amendment value in the 3D CAD files.

a. *Karn v. United States Department of State*

Phillip Karn sought permission to export the book *Applied Cryptography* by Bruce Schneier outside the United States.²⁶² The book included the source code for an encryption algorithm, both in a printed format and on an attached computer diskette.²⁶³ The government determined that the book was not subject to the jurisdiction of ITAR, but the diskette was designated as a protected “munition.”²⁶⁴ (Though, it is reassuring that the government is not arguing here, as it has elsewhere, that it has the power to ban a book.²⁶⁵) The District Court for the District of Columbia dismissed

258. *See id.* at 4.

259. *See Bernstein v. U.S. Dep’t of Justice*, 176 F.3d 1132, 1141, 1143–45 (9th Cir.), *reh’g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

260. *See Junger v. Daley*, 209 F.3d 481, 483 (6th Cir. 2000).

261. *See id.* at 482.

262. *See Karn*, 925 F. Supp. at 4.

263. *See id.*

264. *See id.*

265. *See* Oral Argument at 31:04, *Citizens United v. Fed. Election Comm’n*, 558 U.S. 310 (No. 08-205), *available at* http://www.oyez.org/cases/2000-2009/2008/2008_08_205 (Deputy Solicitor General Malcolm Stewart conceding that the government could ban a book under campaign finance law); *see also* Jonathan H. Adler, *Jeffrey Toobin on Citizens United, VOLOKH CONSPIRACY* (May 14, 2012 9:53 PM), <http://www.volokh.com/2012/05/14/jeffrey-toobin-on-citizens-united/>. Fortunately, during re-argument, then-Solicitor General Elena Kagan made clear the government could not ban a book. *See* Richard L. Hasen, *The Big Ban Theory*, SLATE (May 24, 2010 12:16 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2010/05/the_big_ban_theory.html.

Karn's First Amendment challenge.²⁶⁶ First, the court "assume[d] that the protection of the First Amendment extends to the source code and [explanatory] comments on the plaintiff's diskette."²⁶⁷ Though, it stressed in a footnote that "[t]he Court makes no ruling as to whether source codes, without the comments, fall within the protection of the First Amendment. Source codes are merely a means of commanding a computer to perform a function."²⁶⁸

Second, the court found that the regulation was content-neutral: the government was "not regulating the export of the diskette because of the expressive content of the comments and or source code, but instead . . . because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications."²⁶⁹ After determining that the regulation was content-neutral, the court concluded that, under the under the intermediate scrutiny of the *O'Brien* test, it was valid.²⁷⁰

The court refused to "delve" into the policy dispute of whether the government correctly listed the algorithm on ITAR, even though "cryptographic algorithms contained on the Karn diskette are already widely available in other countries [through the Internet and other sources] or are so 'weak' that they can be broken by the [National Security Agency]."²⁷¹ That something is in the public domain, and is readily available, does not suggest a lack of narrow tailoring on the part of the executive branch.²⁷² The court was not willing to "scrutinize the actual injury to national security" by allowing the export of these algorithms.²⁷³

In the end, the court concluded "that the regulation of the plaintiff's diskette is narrowly tailored to the goal of limiting the proliferation of cryptographic products and that the regulation is

266. See *Karn*, 925 F. Supp. at 3.

267. *Id.* at 9.

268. *Id.* at 9 n.19.

269. *Id.* at 10.

270. See *id.* at 9 ("The[] . . . criteria [that a] regulation is (1) within the constitutional power of the government, (2) 'furthers an important or substantial governmental interest,' and (3) is narrowly tailored to the governmental interest—have been referred to as the *O'Brien* test after the Supreme Court upheld the government's prohibition against burning draft cards based on these criteria in [*United States v. O'Brien*, 391 U.S. 367 (1968)].").

271. *Id.* at 11.

272. See *id.* at 10–11.

273. *Id.* at 12 (citing *United States v. Martinez*, 904 F.2d 601, 602 (11th Cir. 1990)).

justified.”²⁷⁴ Following an appeal, the D.C. Circuit Court of Appeals reversed and remanded the case after President Clinton issued an “Executive Order transferring regulatory authority of non-military cryptographic computer source code to the Commerce Department, and the Commerce Department’s promulgation of a new regulation under the authority of the International Emergency Economic Powers Act.”²⁷⁵ This effectively mooted the case.

b. Bernstein v. U.S. Department of Justice

Bernstein is a bear of a case, with a tortured procedural posture. Professor Daniel Bernstein sought permission to publish “The Snuffle Encryption System” in two forms: a paper containing analysis of the algorithm and the source code of algorithm written in the “C” programming language.²⁷⁶ The State Department authorized Bernstein to publish the written paper, but it classified the source code of the algorithm as a “munition under the International Traffic in Arms Regulations” and required that Bernstein register for a license to “export” the source code.²⁷⁷ Bernstein challenged the licensing scheme imposed by ITAR as a prior restraint on free speech in violation of the First Amendment.²⁷⁸

In a scholarly treatment of the subject, Judge Betty Fletcher, on appeal, found that the government’s enforcement of ITAR violated the First Amendment.²⁷⁹ The *Bernstein* court “conclude[d] that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for

274. *Id.*

275. *Karn v. U.S. Dep’t of State*, 107 F.3d 923 (D.C. Cir. 1997) (per curiam). To the extent that ITAR derives any of its statutory authority from legislation implementing a treaty, that would not give Congress additional power to violate provisions in the Bill of Rights, such as the First and Second Amendments. *See Reid v. Covert*, 354 U.S. 1, 5 (1957) (“At the beginning we reject the idea that when the United States acts against citizens abroad it can do so free of the Bill of Rights.”); *see also* Josh Blackman, *Regulating the Second Amendment Through the Treaty Power*, JOSH BLACKMAN’S BLOG (Feb. 7, 2013), <http://joshblackman.com/blog/2013/02/07/regulating-the-second-amendment-through-the-treaty-power/>.

276. *See Bernstein v. U.S. Dep’t of Justice*, 176 F.3d 1132, 1135–36 (9th Cir.), *reh’g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

277. *Id.* at 1136.

278. *See id.*

279. *See id.* at 1147.

First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine.”²⁸⁰

The government’s arguments, which the Ninth Circuit systematically rejected, are instructive. The government did not “seriously dispute that source code is used by cryptographers for expressive purposes.”²⁸¹ Interestingly, the *Bernstein* court noted that the government acknowledged that “blueprints” are a form of expression (this concession would not bode well for their position on 3D CAD files).²⁸² Instead, the Department of State argued that source code is different from other expressive content because it “can be used to control directly the operation of a computer without conveying information to the user.”²⁸³ To the government, it was the “unique functional aspect of source code,” that defined it, rather than the “content of the ideas that may be expressed.”²⁸⁴ By this logic, the “export regulations manage to skirt entirely the concerns of the First Amendment.”²⁸⁵ The court found this argument “flawed for at least two reasons.”²⁸⁶

First, source code is “written in a language intended also for human analysis and understanding,” in addition to its ability to be compiled into object code which can be read solely by the computer.²⁸⁷ Second, the court rejected the government’s argument that “even one drop of ‘direct functionality’ overwhelms any constitutional protections that expression might otherwise enjoy.”²⁸⁸ The First Amendment, Judge Fletcher found, “is concerned with expression, and . . . the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution” is incorrect.²⁸⁹ Though the CAD files are certainly functional, they also have a strong expressive element that warrants First Amendment protection. The court did narrow its opinion, though, stressing that not all source code is protected by the First Amendment: “We do not hold that all software is expressive. Much of it surely is not.”²⁹⁰

280. *Id.* at 1141.

281. *Id.*

282. *See id.* at 1142.

283. *Id.* at 1141–42.

284. *Id.* at 1142.

285. *Id.*

286. *Id.*

287. *Id.*

288. *Id.*

289. *Id.*

290. *See id.* at 1145.

Professor Eugene Volokh views source code as protected by the First Amendment regardless of whether it is viewed as functional or not.²⁹¹ If source code restrictions are viewed as “restrictions on the functional aspect of the code (since the code can be directly compiled into object code and executed, without a human reading it) rather than the expressive aspect,” then the “human-language descriptions of the algorithm that the source code embodies” would be protected.²⁹²

As a result, the government’s application of ITAR enforcement, as applied to the cryptography algorithm “allow[s] the government to restrain speech indefinitely with no clear criteria for review” and “scientists have been effectively chilled from engaging in valuable scientific expression.”²⁹³ In conclusion, “because the challenged regulations grant boundless discretion to government officials, and because they lack the required procedural protections,” the court found that “they operate as an unconstitutional prior restraint on speech.”²⁹⁴

Alas, the precedential value of *Bernstein* is bare. On September 30, 1999, the court granted the government’s petition for rehearing en banc, and withdrew the published opinion.²⁹⁵ The case fizzled out following a remand after the government no longer sought to enforce the regulation against Bernstein.²⁹⁶

c. *Junger v. Daley*

Peter Junger, a law professor at Case Western University School of Law, sought to “post on his web site encryption source code that he has written to demonstrate how computers work.”²⁹⁷ The code was meant as a teaching tool for his students.²⁹⁸ The government determined that, similar to *Karn* and *Bernstein*, Junger’s “printed book chapter containing encryption code could be exported” but that

291. See Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1222 (2005).

292. *Id.* at 1222.

293. *Bernstein*, 176 F.3d at 1145.

294. *Id.*

295. *Bernstein v. U.S. Dep’t of Justice*, 192 F.3d 1308, 1308 (9th Cir. 1999) (order).

296. See D.J. Bernstein, *Summary of the Case Status*, CR.YP.TO, <http://cr.yp.to/export/status.html> (last visited May 31, 2014).

297. *Junger v. Daley*, 209 F.3d 481, 483 (6th Cir. 2000).

298. See *id.*

the “export of the book in electronic form would require a license.”²⁹⁹ Junger claimed that the “encryption source code is protected speech.”³⁰⁰ The district court opinion, which was issued after *Karn* was remanded and while *Bernstein* was being appealed to the Ninth Circuit, found that the “subject regulations [was] content neutral” and survived intermediate scrutiny.³⁰¹

In *Junger v. Daley*, the Sixth Circuit rejected the claim that the government could restrict the exportation of encryption software, finding that “First Amendment protects computer source code.”³⁰² After determining that “computer source code is an expressive means for the exchange of information and ideas about computer programming,” Judge Martin held that “it is protected by the First Amendment.”³⁰³ The court added a caveat to the holding, however, finding that “national security interests can outweigh the interests of protected speech and require the regulation of speech.”³⁰⁴

While disentangling the “functional” and “expressive” nature of cryptographic source code, the court observed that “source code is the most efficient and precise means by which to communicate ideas about cryptography.”³⁰⁵ The Sixth Circuit rejected the district court’s characterization that “the functional characteristics of source code overshadow its simultaneously expressive nature” and stressed that the “fact that a medium of expression has a functional capacity should not preclude constitutional protection.”³⁰⁶

The First Amendment protects “symbolic conduct, such as draft-card burning, that has both functional and expressive features.”³⁰⁷ The court analogized a “a musical score” —clearly protected by the First Amendment—that “cannot be read by the majority of the public but can be used as a means of communication among musicians” to “computer source code, though unintelligible to many, is the preferred method of communication among computer programmers.”³⁰⁸ Therefore, “computer source code is an expressive

299. *Id.* at 484.

300. *Id.*

301. *Junger v. Daley*, 8 F. Supp. 2d 708, 720 (N.D. Ohio 1998) *rev’d*, 209 F.3d 481 (6th Cir. 2000).

302. *Junger*, 209 F.3d at 482.

303. *Id.* at 485.

304. *Id.*

305. *Id.* at 484.

306. *Id.*

307. *Id.* (citing *United States v. O’Brien*, 391 U.S. 367 (1968)).

308. *Id.*

means for the exchange of information and ideas about computer programming, [and] it is protected by the First Amendment.”³⁰⁹

Noting that intermediate scrutiny applies under the *O'Brien* test, the court found that the “record does not resolve whether the exercise of presidential power in furtherance of national security interests should overrule the interests in allowing the free exchange of encryption source code.”³¹⁰ The court remanded the case to the district court to consider the impact of “recent amendments to the Export Administration Regulations” on Junger’s constitutional claim.³¹¹ This case also fizzled out on remand, apparently due to a lack of enforcement. Sensing a pattern?

2. Unliberating the Liberator

On May 8, 2013, the U.S. Department of State’s Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance, unliberated the Liberator.³¹² In a letter to Cody Wilson, the Office’s Chief Enforcement Officer wrote that “Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.” Citing section 120.10 of ITAR, the letter classified the CAD source files as “information in the form of blueprints” that are forbidden “technical data.”³¹³ (Note how the restricted content is described in terms of “information” and “data”). The letter closed by asking Defense Distributed to submit information concerning ITAR-compliance.³¹⁴ Until that information is submitted, the “technical data [is deemed] ITAR-controlled” and must be “removed from public access immediately.”³¹⁵ That letter shot down the Liberator.

Wilson “complied . . . [i]nstantly,” removing all of the files even though he contested the legality of the order.³¹⁶ He noted that he did not expect the plans to be online for long: “If the Liberator works, it’s only logical that government will fight it.”³¹⁷ Reason Magazine

309. *Id.* at 485.

310. *Id.*

311. *Id.*

312. See Letter from Glenn E. Smith to Cody Wilson, *supra* note 106.

313. *Id.*

314. *Id.*

315. *Id.*

316. Doherty, *supra* note 12.

317. Uwe Buse, *Danger in 3-D: The Rapid Spread of Printable Pistols*, ABC NEWS (June 9, 2013), <http://abcnews.go.com/International/danger-rapid-spread-print>

reported that “[m]aybe the files were acts of free speech, maybe not; Wilson wasn’t going to press the issue just now.”³¹⁸

3. The Constitutionality of ITAR as Applied to 3D Guns

As applied to the Liberator, ITAR restricts speech made in support of the Second Amendment. More precisely, the enforcements constitute a content-based prior restraint on highly-protected speech. With this perspective, the primary right being violated is the right to free speech, which courts have acknowledged is infringed by ITAR. But the derivative or hybrid right, which bolsters free speech, is that the communications are made in pursuance of the right to keep and bear arms. In conjunction with the free speech limitations of ITAR, a heightened scrutiny would apply.

α. ITAR as Content-Based Prior Restraint of Speech

The First Amendment, Judge Fletcher found, “is concerned with expression, and . . . the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution [is incorrect].”³¹⁹ Though the CAD files are certainly functional, they have a strong expressive element that warrants First Amendment protection. The *Bernstein* court’s definition of “source code” is instructive, as it closely resembles the nature of the CAD files used to print 3D guns. “‘Source code,’ at least as currently understood by computer programmers, refers to the text of a program written in a ‘high-level’ programming language.”³²⁰ Source code “is meant to be read and understood by humans and . . . can be used to express an idea or a method.”³²¹ A computer cannot make any “direct use of source code until it has been translated (‘compiled’) into a ‘low-level’ or ‘machine’ language, resulting in computer-executable ‘object code.’”³²² The source code “must follow stringent grammatical, syntactical, formatting, and punctuation conventions” as it is “destined for the maw of an automated, ruthlessly literal translator—the compiler.”³²³

ablepistols/story?id=19348773.

318. Doherty, *supra* note 12.

319. *Bernstein v. U.S. Dep’t of Justice*, 176 F.3d 1132, 1142 (9th Cir.), *reh’g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

320. *Id.* at 1140.

321. *Id.*

322. *Id.*

323. *Id.*

Only those programmers “trained in programming can easily understand source code.”³²⁴ The CAD files closely resemble source code, as described by the *Bernstein* court. Programming source code is compiled to generate object code. CAD files are rendered to generate the 3D files. In much the same way, the CAD files are clearly “intended also for human analysis and understanding.”³²⁵ The source code, once compiled, displays, in vivid three dimensions, the shape and size of the quintessential gun parts used for self-defense. And the CAD rendering program, like the compiler, can translate the vertices and data points in an actual object code, which is then used to 3D print the object.

In *Karn*, the district court agreed with the government that the regulation of the source code was “content-neutral.”³²⁶ The court accepted the government’s rationale “rationale for regulating the export of the diskette is that ‘the proliferation of [cryptographic hardware and software] will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests.’”³²⁷ Judge Richey added:

[The government is] not regulating the export of the diskette because of the expressive content of the comments and or source code, but instead [is] regulating because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications.³²⁸

The district court opinion in *Junger* also found that applying the export control laws to the electronic source code in question was “content-neutral.”³²⁹

The *Bernstein* court declined to decide “whether the challenged regulations constitute content-based restrictions subject to the strictest constitutional scrutiny or whether they are, instead, content-neutral restrictions meriting less exacting scrutiny.”³³⁰ Instead, the Ninth Circuit held that “because the prepublication licensing regime challenged . . . applies directly to scientific

324. *Id.*

325. *Id.* at 1142.

326. *See Karn v. U.S. Dep’t of State*, 925 F. Supp. 1, 10–11 (D.D.C. 1996).

327. *Id.* at 11.

328. *Id.* at 10.

329. *See Junger v. Daley*, 8 F. Supp. 2d 708, 720 (N.D. Ohio 1998), *rev’d*, 209 F.3d 481 (6th Cir. 2000).

330. *Bernstein*, 176 F.3d at 1145.

expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, it constitutes an impermissible prior restraint on speech.”³³¹ The argument that restrictions on these source code files are content-neutral seems rather weak. What the government was regulating was certain types of encryption algorithms.

The State Department’s letter to Cody Wilson makes no reference to the fact that the files being shared are in an electronic format.³³² In fact, it is not even clear if a non-electronic format of the blueprints exists.³³³ Instead, the letter focuses on the content of the “subject technical data” on “DEFCAD.org.”³³⁴ Specifically, it enumerates ten items, based on the subject of their source code:

[The] Department believes Defense Distributed may not have established the proper jurisdiction of the subject technical data:

1. Defense Distributed Liberator Pistol
2. .22 electric
3. 125mm BK-14M high-explosive anti-tank warhead
4. 5.56/.223 muzzle brake
5. Springfield XD-40 tactical slide assembly
6. Sound Moderator – slip on
7. “The Dirty Diane” 1/2-28 to 3/4-16 STP S3600 oil filter
silencer adapter
8. 12 gauge to .22 CB sub-caliber insert
9. Voltlock electronic black powder system
10. VZ-58 front sight.³³⁵

These are all classifications based on the subject of the source code—in particular, what objects the 3D CAD files express. This seems to conflict with the Supreme Court’s pronouncement that, “as a general matter, . . . government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.”³³⁶ Intermediate scrutiny, as the *Karn* and *Junger* district courts applied, is therefore inappropriate.

331. *Id.* at 1143.

332. See Letter from Glenn E. Smith to Cody Wilson, *supra* note 99.

333. See Greenberg, *supra* note 210 (“Wilson . . . says that Defcad’s files have also been made available for sale in an Austin, Texas bookstore that he declined to name in order to protect the bookstore’s owner from scrutiny.”).

334. See Letter from Glenn E. Smith to Cody Wilson, *supra* note 99.

335. *Id.*

336. *Ashcroft v. Am. Civil Liberties Union*, 535 U.S. 564, 573 (2002) (internal quotation marks omitted).

Rather, content-based restrictions of speech, particularly prior restraints, must pass strict scrutiny and be “justified by a compelling government interest and [be] narrowly drawn to serve that interest.”³³⁷ Under strict scrutiny, the government “must specifically identify an ‘actual problem’ in need of solving.”³³⁸ Any “curtailment of free speech must be actually necessary to the solution.”³³⁹ As the Court found in *Brown v. EMA*, “that is a demanding standard,”³⁴⁰ and “[i]t is rare that a regulation restricting speech because of its content will ever be permissible.”³⁴¹

Even if the ITAR regulation is viewed as content-neutral, then the *O’Brien* intermediate scrutiny would be merged with the *Heller* intermediate scrutiny (as determined by the majority of cases).³⁴² What does intermediate plus intermediate result in? *Smith* suggested that something approaching strict scrutiny would be appropriate for hybrid claims.³⁴³

Further, allowing the author to release the expression in book form, and not digital form, would not in the least be narrowly tailored. Practically speaking, a printed version of the source code—which may run in the hundreds of pages—is effectively useless. It would have to be manually re-typed into the computer to render the objects in three-dimensions. The only viable means of using source code is in a digital format. In addition, presumably, if someone were to type all of the source code correctly, once completed, it would be deemed an unlawful munition, and subject to ITAR control. There are no “reasonable alternative avenues of communication.”³⁴⁴ You can’t win. ITAR renders 3D blueprints useless. As applied, ITAR unconstitutionally infringes on both First and Second Amendment rights of Cody Wilson, and those who wanted to learn from that information about the right to keep and bear arms.

337. *Brown v. Entm’t Merchants Ass’n*, 131 S. Ct. 2729, 2738 (2011) (citing *R.A.V. v. St. Paul*, 505 U.S. 377, 395 (1992)).

338. *Id.* (quoting *United States v. Playboy Entm’t Grp., Inc.*, 529 U.S. 803, 822–23 (2000)).

339. *Id.* (citing *R.A.V.*, 505 U.S. at 395).

340. *Id.*

341. *Playboy*, 529 U.S. at 818.

342. See Nelson Lund, *Second Amendment Standards of Review in a Heller World*, 39 *FORDHAM URB. L.J.* 1617, 1622 (2012).

343. See *Employment Div., Dep’t of Human Res. of Or. v. Smith*, 494 U.S. 872, 881–82 (1990).

344. *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 64 (1986).

b. Balancing National Security and the First and Second Amendments

The government's strongest countervailing interest to regulate the CAD files is national security, and the ability to speak with a single voice with respect to foreign affairs.³⁴⁵ As the Court recently explained in upholding a restriction on providing material support to foreign terrorist organizations, "[e]veryone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order," even against a First Amendment challenge.³⁴⁶ For example, in *Karn*, the district court was not willing to "question the logic" of the government's rationale, and would not inquire whether "there is no actual danger to national security because the source codes can be obtained abroad through the book or on the Internet."³⁴⁷

However, under strict scrutiny, this is exactly the type of inquiry that courts must perform. As the Court made clear in the context of cell phone privacy, even if using information in an illicit manner may harm others, data by itself "can endanger no one."³⁴⁸ The Supreme Court has imposed a high burden on the government for content-based prior restraints of speech, even when the asserted interest is national security: "[T]he presumption against prior restraints may be overcome where publication would directly and imminently imperil national security."³⁴⁹ For the government to "justify a prior restraint on national security grounds, the government must prove the publication would 'surely result in direct, immediate, and irreparable damage to our Nation or its people.'"³⁵⁰ Justice Brennan explained that national security is only a valid interest to justify prior restraint when there is "governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred

345. See *United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304, 321 (1936).

346. *Holder v. Humanitarian Law Project*, 561 U.S. 1, 29 (2010).

347. *Karn v. U.S. Dep't of State*, 925 F. Supp. 1, 10 (D.D.C. 1996).

348. *Riley v. California*, 573 U.S. __ (2014).

349. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1144 n.19 (9th Cir.), *reh'g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999) (citing *N.Y. Times Co. v. United States*, 403 U.S. 713, 730 (1971) (Stewart, J., joined by White, J., concurring); *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 715 (1931); *United States v. Progressive, Inc.*, 467 F. Supp. 990, 992 (W.D. Wis. 1979)).

350. *Id.* (quoting *N.Y. Times*, 403 U.S. at 730 (Stewart, J., joined by White, J., concurring)).

to imperiling the safety of a transport already at sea.”³⁵¹ Recently, the Court stressed that merely showing a connection between speech and harming national interests would not be dispositive to satisfy a First Amendment challenge.³⁵² An open-sourced CAD file of a simple pistol that is readily available all over the internet would not even come close to meeting this lofty threshold.

The State Department, in their efforts to stop the distribution of a simple handgun that anyone with basic parts can construct, hardly justifies this burden. To the extent that scientific research is an important facet of the First Amendment, engaging in expression about another constitutional right, the Second Amendment, is of a much higher constitutional order. Further, the handgun is at the core of the Second Amendment, which was the firearm singled out by Justice Scalia in *Heller* as the quintessential self-defense weapon.³⁵³

Relying on the *Pentagon Papers Case* in *Bernstein*, the Ninth Circuit concluded that the government did not, and could not plausibly argue that “prior restraint at issue here falls within the extremely narrow class of cases where publication would directly and immediately imperil national security.”³⁵⁴ When read together with the Second Amendment right to make arms, the government’s countervailing interest in imposing this prior restraint becomes even more untenable under strict scrutiny.

c. *The Regulation of Information*

Cody Wilson, the creator of the Liberator, views the debate in similar terms. On a now-removed FAQ page, Cody Wilson described

351. *N.Y. Times*, 403 U.S. at 726–27 (Brennan, J., concurring).

352. *See Holder*, 561 U.S. at 39 (“All this is not to say that any future applications of the material-support statute to speech or advocacy will survive First Amendment scrutiny. It is also not to say that any other statute relating to speech and terrorism would satisfy the First Amendment. In particular, we in no way suggest that a regulation of independent speech would pass constitutional muster, even if the Government were to show that such speech benefits foreign terrorist organizations. We also do not suggest that Congress could extend the same prohibition on material support at issue here to domestic organizations.”).

353. *See District of Columbia v. Heller*, 554 U.S. 570, 629 (2008) (“There are many reasons that a citizen may prefer a handgun for home defense: It is easier to store in a location that is readily accessible in an emergency; it cannot easily be redirected or wrestled away by an attacker; it is easier to use for those without the upper-body strength to lift and aim a long gun; it can be pointed at a burglar with one hand while the other hand dials the police.”).

354. *Bernstein*, 176 F.3d at 1144 n.19.

the blueprints in terms of speech.³⁵⁵ “Since its inception, it has been legal in the USA to fashion your own firearm, and to talk about doing so Everything else is free speech, ladies and gentlemen.”³⁵⁶ Wilson commented on the fact that ITAR controls not only “actual arms, but technical data.”³⁵⁷ He added, “I don’t like it—but I do think that it actually ends up helping the message of the project a little more, that, look, in the end we’re going to be having a fight about what it means to be controlling information.”

At issue here are the First and Second Amendments. “This is about the future of the freedom of information and regulation of the Internet,” Wilson explained.³⁵⁸ Or, as columnist Brian Doherty put it, “The State Department didn’t say for sure that this information (*some might call it speech*) fell under its jurisdiction.”³⁵⁹ Guns were not the point of Wilson’s project. “This is a fight about two competing visions of the future. I think my vision of distributed technology will win.”³⁶⁰ It is no longer possible to focus on policing the possession and distribution of actual products. Now, the information that creates these products must be censored. Efforts to stifle 3D printing is the next chapter in suppressing information and data on the internet.

CONCLUSION

3D printing holds great potential to revolutionize the way that people invent, create, and use innovative new products. For prudential reasons, the government should resist the siren call of incumbents to regulate and shackle this technology. But more importantly, any efforts to regulate the distribution and use of 3D blueprints must be done with respect for the Constitution. Instituting a flat ban on 3D gun blueprints constitutes a prior restraint, and is a content-based restriction on speech that promotes Second Amendment rights. Though the government has countervailing interests in promoting security, an overbroad ban on all firearm blueprints cannot withstand constitutional scrutiny. In

355. See Josh Blackman, *1, 2, 3: The First and Second Amendments Meet Third Dimensional Printing*, JOSH BLACKMAN’S BLOG (Oct. 22, 2012), <http://joshblackman.com/blog/2012/10/22/1-2-3-the-first-and-second-amendments-meet-third-dimensional-printing/>.

356. See *id.*

357. Murphy, *supra* note 198.

358. Preston, *supra* note 37.

359. Doherty, *supra* note 12.

360. Preston, *supra* note 37.

the end, this technology should flourish, out of respect for innovation, and the Constitution.

As an aside, I was tempted to include the actual source code for The Liberator 3D gun in this Article. However, because this journal will certainly be shared outside the United States, I would likely be required to register it with the State Department as a prohibited munition. Think about that for a moment. There is some irony in the fact that ITAR has chilled my free speech, because I want to discuss how ITAR infringes on free speech. Though, this Article published in print *and* a digital format would have made one heck of a test case.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, ET AL.,	§	
	§	
Plaintiffs,	§	
	§	
V.	§	1-15-CV-372 RP
	§	
UNITED STATES DEPARTMENT OF	§	
STATE, ET AL.,	§	
	§	
Defendants.	§	

ORDER

Before the Court are Plaintiffs' Motion for Preliminary Injunction, filed May 11, 2015 (Clerk's Dkt. #7), Memorandum of Points and Authorities in Support of Plaintiffs' Motion for Preliminary Injunction, filed May 11, 2015 (Clerk's Dkt. #8) and the responsive pleadings thereto. The Court conducted a hearing on the motion on July 6, 2015. Having considered the motion, responsive pleadings, record in the case, and the applicable law, the Court is of the opinion that Plaintiffs' motion for a preliminary injunction should be denied. See FED. R. CIV. P. 65(b).

I. BACKGROUND

Plaintiffs Defense Distributed and the Second Amendment Foundation ("SAF") bring this action against defendants the United States Department of State, Secretary of State John Kerry, the Directorate of Defense Trade Controls ("DDTC"), and employees of the DDTC in their official and individual capacities, challenging implementation of regulations governing the "export" of "defense articles."

Under the Arms Export Control Act ("AECA"), "the President is authorized to control the import and the export of defense articles and defense services" and to "promulgate regulations for the import and export of such articles and services." 22 U.S.C. § 2778(a)(1). The AECA imposes both civil and criminal penalties for violation of its provisions and implementing regulations,

including monetary fines and imprisonment. *Id.* § 2278(c) & (e). The President has delegated his authority to promulgate implementing regulations to the Secretary of State. Those regulations, the International Traffic in Arms Regulation (“ITAR”), are in turn administered by the DDTC and its employees. 22 C.F.R. 120.1(a).

The AECA directs that the “defense articles” designated under its terms constitute the United States “Munitions List.” 22 U.S.C. § 2278(a)(1). The Munitions List “is not a compendium of specific controlled items,” rather it is a “series of categories describing the kinds of items” qualifying as “defense articles.” *United States v. Zhen Zhou Wu*, 711 F.3d 1, 12 (1st Cir.) *cert. denied sub nom. Yufeng Wei v. United States*, 134 S. Ct. 365 (2013). Put another way, the Munitions List contains “attributes rather than names.” *United States v. Pulungan*, 569 F.3d 326, 328 (7th Cir. 2009) (explaining “an effort to enumerate each item would be futile,” as market is constantly changing). The term “defense articles” also specifically includes “technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in” the Munitions List. 22 C.F.R. § 120.6

A party unsure about whether a particular item is a “defense article” covered by the Munitions List may file a “commodity jurisdiction” request with the DDTC. See 22 C.F.R. § 120.4 (describing process). The regulations state the DDTC “will provide a preliminary response within 10 working days of receipt of a complete request for commodity jurisdiction.” *Id.* § 120.4(e). If a final determination is not provided after 45 days, “the applicant may request in writing to the Director, Office of Defense Trade Controls Policy that this determination be given expedited processing.” *Id.*

According to Plaintiffs, Defense Distributed publishes files on the Internet as a means of fulfilling its primary missions to promote the right to keep and bear arms and to educate the public, as well as generating revenue. Specifically, in December 2012 Defense Distributed made available for free on the Internet privately generated technical information regarding a number of gun-related

items (the “Published Files”). (Compl. ¶¶ 22-24). Plaintiffs allege that, on May 8, 2013, Defendants sent Defense Distributed a letter stating:

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEF CAD.org, the majority of which appear to be related to items in Category I of the [Munitions List]. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

(*Id.* ¶ 25).

Plaintiffs state they promptly removed the Published Files from the Internet. Further, per instruction in the May 2013 letter, Plaintiffs submitted commodity jurisdiction requests covering the Published Files on June 21, 2013. According to Plaintiffs, they have not received a response to the requests from Defendants. (*Id.* ¶¶ 26-29).

Plaintiffs further allege that, on September 25, 2014, Defense Distributed sent a request for prepublication approval for public release of files containing technical information on a machine named the “Ghost Gunner” that can be used to manufacture a variety of items, including gun parts (the “Ghost Gunner Files”).¹ Following resubmission of the request, on April 13, 2015, DDTC determined that the Ghost Gunner machine, including the software necessary to build and operate the Ghost Gunner machine, is not subject to ITAR, but that “software, data files, project files, coding, and models for producing a defense article, to include 80% AR-15 lower receivers, are subject to the jurisdiction of the Department of State in accordance with [ITAR].” (*Id.* ¶¶ 28-33).

In addition, Plaintiffs allege that since September 2, 2014, Defense Distributed has made multiple requests to DOPSR for prepublication review of certain computer-aided design (“CAD”) files. In December 2014, DOPSR informed Defense Distributed that it refused to review the CAD files. The DOPSR letter directed Defense Distributed to the DDTC Compliance and Enforcement

¹ According to Plaintiffs, Defendants identify the Department of Defense Office of Prepublication Review and Security (“DOPSR”) as the government agency from which private persons must obtain prior approval for publication of privately generated technical information subject to ITAR control. (Compl. ¶ 28).

Division for further questions on public release of the CAD files. Defense Distributed has sought additional guidance on the authorization process, but to date, Defendants have not responded. (*Id.* ¶¶ 34-36).

Plaintiffs filed this action on April 29, 2015, raising five separate claims. Specifically, Plaintiffs assert that the imposition by Defendants of a prepublication approval requirement for “technical data” related to “defense articles” constitutes: (1) an ultra vires government action; (2) a violation of their rights to free speech under the First Amendment; (3) a violation of their right to keep and bear arms under the Second Amendment; and (4) a violation of their right to due process of law under the Fifth Amendment. Plaintiffs also contend the violations of their constitutional rights entitled them to monetary damages under *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971). Plaintiffs now seek a preliminary injunction enjoining the enforcement of any prepublication approval requirement against unclassified information under the ITAR, specifically including all files Defense Distributed has submitted for DOPSR review. The parties have filed responsive pleadings. The Court conducted a hearing on July 6, 2015 and the matter is now ripe for review.

II. STANDARD OF REVIEW

A preliminary injunction is an extraordinary remedy and the decision to grant a preliminary injunction is to be treated as the exception rather than the rule. *Valley v. Rapides Parish Sch. Bd.*, 118 F.3d 1047, 1050 (5th Cir. 1997). The party seeking a preliminary injunction may be granted relief *only* if the moving party establishes: (1) a substantial likelihood of success on the merits; (2) a substantial threat that failure to grant the injunction will result in irreparable injury; (3) that the threatened injury out-weighs any damage that the injunction may cause the opposing party; and (4) that the injunction will not disserve the public interest. *See Hoover v. Morales*, 146 F.3d 304, 307 (5th Cir.1998); *Wenner v. Texas Lottery Comm'n*, 123 F.3d 321, 325 (5th Cir. 1997); *Cherokee*

Pump & Equip. Inc. v. Aurora Pump, 38 F.3d 246, 249 (5th Cir. 1994). To show a substantial likelihood of success, “the plaintiff must present a prima facie case, but need not prove that he is entitled to summary judgment.” *Daniels Health Sciences, L.L.C. v. Vascular Health Sciences, L.L.C.*, 710 F.3d 579, 582 (5th Cir. 2013). See also *Janvey v. Alguire*, 647 F.3d 585, 596 (5th Cir. 2011) (same, citing CHARLES ALAN WRIGHT, ARTHUR R. MILLER, MARY KAY KANE, 11A FEDERAL PRACTICE & PROCEDURE § 2948.3 (2d ed. 1995) (“All courts agree that plaintiff must present a prima facie case but need not show that he is certain to win.”)). The party seeking a preliminary injunction must clearly carry the burden of persuasion on all four requirements to merit relief. *Mississippi Power & Light Co.*, 760 F.2d 618, 621 (5th Cir. 1985).

III. ANALYSIS

Defendants maintain Plaintiffs have not established any of the four requirements necessary to merit grant of a preliminary injunction. Plaintiffs, of course, disagree. The Court will briefly address the parties’ arguments concerning the final three requirements before turning to the core, and dispositive question, whether Plaintiffs have shown a likelihood of success on the merits of their claims.

A. Injury and Balancing of Interests

Defendants suggest Plaintiffs’ contention that they face irreparable injury absent immediate relief is rebutted by their delay in filing this lawsuit. However, the Supreme Court has stated that the “loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.” *Elrod v. Burns*, 427 U.S. 347, 373 (1976); see also *Palmer v. Waxahachie Indep. Sch. Dist.*, 579 F.3d 502, 506 (5th Cir. 2009) (the “loss of First Amendment freedoms for even minimal periods of time constitutes irreparable injury justifying the grant of a preliminary injunction.”). The Second Amendment protects “similarly intangible and unquantifiable interests” and a deprivation is thus considered irreparable. *Ezell v. City of Chicago*, 651 F.3d 684,

699 (7th Cir. 2011) (“for some kinds of constitutional violations, irreparable harm is presumed”). The Court thus has little trouble concluding Plaintiffs have shown they face a substantial threat of irreparable injury.

The Court has much more trouble concluding Plaintiffs have met their burden in regard to the final two prongs of the preliminary injunction inquiry. Those prongs require weighing of the respective interests of the parties and the public. Specifically, that the threatened injury out-weighs any damage that the injunction may cause the opposing party and that the injunction will not disserve the public interest. In this case, the inquiry essentially collapses because the interests asserted by Defendants are in the form of protecting the public by limiting access of foreign nationals to “defense articles.”

Plaintiffs rather summarily assert the balance of interests tilts in their favor because “[I]t is always in the public interest to prevent the violation of a party’s constitutional rights.” *Awad v. Ziriax*, 670 F.3d 1111, 1132 (10th Cir. 2012); *see also Jackson Women’s Health Org. v. Currier*, 760 F.3d 448, 458 n.9 (5th Cir. 2014) (district court did not abuse its discretion in finding injunction would not disserve public interest because it will prevent constitutional deprivations). They further assert that an injunction would not bar Defendants from controlling the export of classified information.

The Court finds neither assertion wholly convincing. While Plaintiffs’ assertion of a public interest in protection of constitutional rights is well-taken, it fails to consider the public’s keen interest in restricting the export of defense articles. *See Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 24-25 (2008) (discussing failure of district court to consider injunction’s adverse impact on public interest in national defense); *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 826 (2nd Cir. 2015) (characterizing maintenance of national security as “public interest of the highest order”). It also fails to account for the interest – and authority – of the President and Congress in matters of foreign policy and export. *See Haig v. Agee*, 453 U.S. 280, 292 (1981) (matters relating to

conduct of foreign relations “are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference”); *United States v. Pink*, 315 U.S. 203, 222–23 (1942) (conduct of foreign relations “is committed by the Constitution to the political departments of the Federal Government”); *Spectrum Stores, Inc. v. Citgo Petroleum Corp.*, 632 F.3d 938, 950 (5th Cir. 2011) (matters implicating foreign relations and military affairs generally beyond authority of court’s adjudicative powers).

As to Plaintiff’s second contention, that an injunction would not bar Defendants from controlling the export of classified information, it is significant that Plaintiffs maintain the posting of files on the Internet for free download does not constitute “export” for the purposes of the AECA and ITAR. But Defendants clearly believe to the contrary. Thus, Plaintiffs’ contention that the grant of an injunction permitting them to post files that Defendants contend are governed by the AECA and ITAR would not bar Defendants from controlling “export” of such materials stand in sharp contrast to Defendants’ assertion of the public interest. The Court thus does not believe Plaintiffs have met their burden as to the final two prongs necessary for granting Plaintiffs a preliminary injunction. Nonetheless, in an abundance of caution, the Court will turn to the core of Plaintiffs’ motion for a preliminary injunction, whether they have shown a likelihood of success on their claims

B. Ultra Vires

Plaintiffs first argue Defendants are acting beyond the scope of their authority in imposing a prepublication requirement on them under the AECA. A federal court has no subject matter jurisdiction over claims against the United States unless the government waives its sovereign immunity and consents to suit. *Danos v. Jones*, 652 F.3d 577, 581 (5th Cir. 2011) (citing *FDIC v. Meyer*, 510 U.S. 471, 475 (1994)). The ultra vires exception to sovereign immunity provides that “where the officer’s powers are limited by statute, his actions beyond those limitations are considered individual and not sovereign actions,” or “ultra vires his authority,” and thus not

protected by sovereign immunity. *Larson v. Domestic & Foreign Commerce Corp.*, 337 U.S. 682, 689 (1949). To fall within the ultra vires exception to sovereign or governmental immunity, a plaintiff must “do more than simply allege that the actions of the officer are illegal or unauthorized.” *Danos*, 652 F.3d at 583. Rather, the complaint must allege facts sufficient to establish that the officer was acting “without any authority whatever,” or without any “colorable basis for the exercise of authority.” *Id.* (quoting *Pennhurst State Sch. & Hosp. v. Halderman*, 465 U.S. 89, 101 n.11 (1984)).

The statute at issue provides:

In furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services.

22 U.S.C. § 2778(a)(1). “Export” is defined, in pertinent part, as including “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person whether in the United States or abroad.” 22 C.F.R. § 120.17(a)(4). Plaintiffs argue this definition falls outside Congressional intent in authorizing restriction of export of defense articles because, as interpreted by Defendants, it includes public speech within the United States.

Notably, Plaintiffs do not suggest Defendants lack authority under the AECA to regulate export of defense articles. Further, under the AECA, decisions are required to

take into account whether the export of an article would contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements.

22 U.S.C. § 2778(a)(2). Defense Distributed admits its purpose is “facilitating *global* access to, and the collaborative production of, information and knowledge related to the three-dimensional (“3D”) printing of arms.” (Compl. ¶ 1) (emphasis added). Facilitating global access to firearms

undoubtedly “increase[s] the possibility of outbreak or escalation of conflict.” Defense Distributed, by its own admission, engages in conduct which Congress authorized Defendants to regulate. Plaintiffs have not, therefore, shown Defendants are acting without any “colorable basis for the exercise of authority.” Accordingly, they have not shown a likelihood of success on their ultra vires challenge.

C. First Amendment

Plaintiffs next argue Defendants’ interpretation of the AECA violates their First Amendment right to free speech. In addressing First Amendment claims, the first step is to determine whether the claim involves protected speech, the second step is to identify the nature of the forum, and the third step is to assess whether the justifications for exclusion from the relevant forum satisfy the requisite standard. *Cornelius v. NAACP Legal Defense & Educ. Fund, Inc.*, 473 U.S. 788, 797 (1985).

As an initial matter, Defendants argue the computer files at issue do not constitute speech and thus no First Amendment protection is afforded. First Amendment protection is broad, covering “works which, taken as a whole, have serious literary, artistic, political, or scientific value, regardless of whether the government or a majority of the people approve of the ideas these works represent.” *Miller v. California*, 413 U.S. 15, 34 (1973). *See also Brown v. Entm’t Merchants Ass’n*, 131 S. Ct. 2729, 2733 (2011) (video games’ communication of ideas and social messages suffices to confer First Amendment protection). Defendants, however, maintain the computer files at the heart of this dispute do not warrant protection because they consist merely of directions to a computer. In support, they rely on a Second Circuit opinion which held that computer instructions that “induce action without the intercession of the mind or the will of the recipient” are not constitutionally protected speech. *Commodity Futures Trading Comm’n v. Vartuli*, 228 F.3d 94, 111 (2nd Cir. 2000).

As Plaintiffs point out, one year later, the Second Circuit addressed the issue of whether computer code constitutes speech at some length in *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2nd Cir. 2001).² The court made clear the fact that computer code is written in a language largely unintelligible to people was not dispositive, noting Sanskrit was similarly unintelligible to many, but a work written in that language would nonetheless be speech. Ultimately, the court concluded “the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions ‘speech’ for purposes of the First Amendment.” *Id.* at 447 (discussing other examples of “instructions” which qualified as speech under First Amendment). Similarly, the Sixth Circuit has found “[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming . . . it is protected by the First Amendment,” even though such code “has both an expressive feature and a functional feature.” *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000).

Although the precise technical nature of the computer files at issue is not wholly clear to the Court, Plaintiffs made clear at the hearing that Defense Distributed is interested in distributing the files as “open source.” That is, the files are intended to be used by others as a baseline to be built upon, altered and otherwise utilized. Thus, at least for the purpose of the preliminary injunction analysis, the Court will consider the files as subject to the protection of the First Amendment.

In challenging Defendants’ conduct, Plaintiffs urge this Court to conclude the ITAR’s imposition of a prepublication requirement constitutes an impermissible prior restraint. Prior restraints “face a well-established presumption against their constitutionality.” *Marceaux v. Lafayette City-Parish Consol. Gov’t*, 731 F.3d 488, 493 (5th Cir. 2013). *See also Organization for*

² Defendants are correct that the *Corley* court did not overrule the decision in *Vartuli*. However, the *Corley* court itself distinguished the decision in *Vartuli* as limited, because it was based on the manner in which the code at issue was marketed. That is, the defendants themselves marketed the software as intended to be used “mechanically” and “without the intercession of the mind or the will of the recipient.” *Corley*, 273 F.3d at 449 (quoting *Vartuli*, 228 F.3d at 111). Plaintiffs here have not so marketed or described the files at issue.

a Better Austin v. Keefe, 402 U.S. 415, 419 (1971) (“Any prior restraint on expression comes ... with a ‘heavy presumption’ against its constitutional validity”); *Shuttlesworth v. City of Birmingham*, 394 U.S. 147, 150–51 (1969) (noting “the many decisions of this Court over the last 30 years, holding that a law subjecting the exercise of First Amendment freedoms to the prior restraint of a license without narrow, objective, and definite standards to guide the licensing authority, is unconstitutional”). “[A] system of prior restraint avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system.” *Collins v. Ainsworth*, 382 F.3d 529, 539 (5th Cir. 2004) (quoting *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 559 (1975)).

The “heavy presumption” against constitutional validity of prior restraint is not, however, “a standard of review, and judicial decisions analyzing prior restraints have applied different standards of review depending on the restraint at issue.” *Catholic Leadership Coal. of Tex. v. Reisman*, 764 F.3d 409, 438 (5th Cir. 2014). See, e.g., *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 33 (1984) (order prohibiting dissemination of discovered information before trial “is not the kind of classic prior restraint that requires exacting First Amendment scrutiny”); *Perry v. McDonald*, 280 F.3d 159, 171 (2nd Cir. 2001) (context in which prior restraint occurs affects level of scrutiny applied);, 192 F.3d 742, 749 (7th Cir. 1999) (“We note initially that the [plaintiff] is simply wrong in arguing that all prior restraints on speech are analyzed under the same test.”).

No party suggests posting of information on the Internet for general free consumption is not a public forum. The next inquiry is thus the applicable level of protection afforded to the files at issue. Content-neutral restrictions on speech are examined under intermediate scrutiny, meaning they are permissible so long as they are narrowly tailored to serve a significant governmental interest and leave open ample alternative channels for communication of the information. *Turner Broad. Sys. v. FCC*, 520 U.S. 180, 213–14 (1997); *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989). Content-based restrictions are examined under strict scrutiny, meaning they must be

narrowly drawn to effectuate a compelling state interest. *Perry Educ. Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37, 46 (1983).

Not surprisingly, the parties disagree as to whether the ITAR imposes content-based restrictions. “Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed.” *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015). Plaintiffs here argue, because the regulations restrict speech concerning the entire topic of “defense articles” the regulation is content-based. “A regulation is not content-based, however, merely because the applicability of the regulation depends on the content of the speech.” *Asgeirsson v. Abbott*, 696 F.3d 454, 459 (5th Cir. 2012). Rather, determination of whether regulation of speech is content-based “requires a court to consider whether a regulation of speech ‘on its face’ draws distinctions based on the message a speaker conveys.” *Reed*, 135 S. Ct. at 2227. *See also Ward*, 491 U.S. at 791 (principal inquiry in determining content-neutrality, “is whether the government has adopted a regulation of speech because of disagreement with the message it conveys”).

Employing this inquiry, the Supreme Court has found regulations to be content-neutral where the regulations are aimed not at suppressing a message, but at other “secondary effects.” For example, the Supreme Court upheld a zoning ordinance that applied only to theaters showing sexually-explicit material, reasoning the regulation was content-neutral because it was not aimed at suppressing the erotic message of the speech but instead at the crime and lowered property values that tended to accompany such theaters. *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 47–48 (1986). The Supreme Court similarly upheld a statute establishing buffer zones only at clinics that performed abortions, concluding the statute did not draw content-based distinctions as enforcement authorities had no need to examine the content of any message conveyed and the stated purpose of the statute was public safety. *McCullen v. Coakley*, 134 S. Ct. 2518, 2531 (2014) (noting violation of statute depended not “on what they say,” but “simply on where they say it”). The

Fifth Circuit has likewise found regulations content-neutral, even where the regulation governed a specific topic of speech. See *Kagan v. City of New Orleans*, 753 F.3d 560, 562 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1403 (2015) (upholding regulation requiring license for a person to charge for tours to City's points of interest and historic sites, "for the purpose of explaining, describing or generally relating the facts of importance thereto," finding regulation "has no effect whatsoever on the content of what tour guides say"); *Asgeirsson*, 696 F.3d at 461 (holding Texas' Open Meeting Act, prohibiting governmental body from conducting closed meetings during which public business or public policy over which the governmental body has supervision or control is discussed, to be content-neutral, because closed meetings: (1) prevent transparency; (2) encourage fraud and corruption; and (3) foster mistrust in government).

The ITAR, on its face, clearly regulates disclosure of "technical data" relating to "defense articles." The ITAR thus unquestionably regulates speech concerning a specific topic. Plaintiffs suggest that is enough to render the regulation content-based, and thus invoke strict scrutiny. Plaintiffs' view, however, is contrary to law. The Fifth Circuit rejected a similar test, formulated as "[a] regulatory scheme that requires the government to 'examine the content of the message that is conveyed' is content-based regardless of its motivating purpose," finding the proposed test was contrary to both Supreme Court and Fifth Circuit precedent. *Asgeirsson*, 696 F.3d at 460.

The ITAR does not regulate disclosure of technical data based on the message it is communicating. The fact that Plaintiffs are in favor of global access to firearms is not the basis for regulating the "export" of the computer files at issue. Rather, the export regulation imposed by the AECA is intended to satisfy a number of foreign policy and national defense goals, as set forth above. Accordingly, the Court concludes the regulation is content-neutral and thus subject to intermediate scrutiny. See *United States v. Chi Mak*, 683 F.3d 1126, 1135 (9th Cir. 2012) (finding the AECA and its implementing regulations are content-neutral).

The Supreme Court has used various terminology to describe the intermediate scrutiny

standard. *Compare Ward*, 491 U.S. at 798 (“a regulation of the time, place, or manner of protected speech must be narrowly tailored to serve the government's legitimate, content-neutral interests but that it need not be the least restrictive or least intrusive means of doing so”), with *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989) (requiring “the government goal to be substantial, and the cost to be carefully calculated,” and holding “since the State bears the burden of justifying its restrictions, it must affirmatively establish the reasonable fit we require”), and *Turner*, 520 U.S. at 189 (regulation upheld under intermediate scrutiny if it “further[s] an important or substantial governmental interest unrelated to the suppression of free speech, provided the incidental restrictions d[o] not burden substantially more speech than is necessary to further those interests”). The Court will employ the Fifth Circuit’s most recent enunciation of the test, under which a court must sustain challenged regulations “if they further an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.” *Time Warner Cable, Inc. v. Hudson*, 667 F.3d 630, 641 (5th Cir. 2012)

The Court has little trouble finding there is a substantial governmental interest in regulating the dissemination of military information. Plaintiffs do not suggest otherwise. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) (noting all parties agreed government's interest in combating terrorism “is an urgent objective of the highest order”). Nor do Plaintiffs suggest the government's regulation is directed at suppressing free expression. Rather, they contend the regulations are not sufficiently tailored so as to only incidentally restrict their freedom of expression.

The only circuit to address whether the AECA and ITAR violate the First Amendment has concluded the regulatory scheme survives such a challenge. In so doing, the Ninth Circuit concluded the technical data regulations substantially advance the government's interest, unrelated to the suppression of expression, because the regulations provide clear procedures for seeking

necessary approval. *Chi Mak*, 683 F.3d at 1135 (citing 22 C.F.R § 120.10(a) (the determination of designation of articles or services turns on whether an item is “specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability such that control under this subchapter is necessary”)). The Ninth Circuit also concluded the regulations were not more burdensome than necessary, noting the “ITAR makes a point to specifically exclude numerous categories from designation, such as general scientific, mathematical, or engineering papers.” *Id.* (citing *Humanitarian Law Project*, 561 U.S. at 29 (upholding material support statute against First Amendment challenge where the statute provided narrowing definitions to avoid infringing upon First Amendment interests)).³

Plaintiffs’ challenge here is based on their contention that Defendants have applied an overbroad interpretation of the term “export.” Specifically, Plaintiffs argue that viewing “export” as including public speech, including posting of information on the Internet, imposes a burden on expression which is greater than is essential to the furtherance of the government’s interest in protecting defense articles.

But a prohibition on Internet posting does not impose an insurmountable burden on Plaintiffs’ domestic communications. This distinction is significant because the AECA and ITAR do not prohibit domestic communications. As Defendants point out, Plaintiffs are free to disseminate the computer files at issue domestically in public or private forums, including via the mail or any other medium that does not provide the ability to disseminate the information internationally.

Nor is the Court convinced by Plaintiffs’ suggestion that the ban on Internet posting does not prevent dissemination of technical data outside national borders, and thus does not further the

³ The Ninth Circuit has also rejected a First Amendment challenge to the AECA’s predecessor, the Mutual Security Act of 1954. *See United States v. Edler Indus., Inc.*, 579 F.2d 516, 521 (9th Cir. 1978) (holding statute and regulations not overbroad in controlling conduct of assisting foreign enterprises to obtain military equipment and related technical expertise and licensing provisions of statute not an unconstitutional prior restraint on speech).

government's interests under the AECA. The Ninth Circuit addressed and rejected a similar suggestion, namely that the only way the government can prevent technical data from being sent to foreign persons is to suppress the information domestically as well, explaining:

This outcome would blur the fact that national security concerns may be more sharply implicated by the export abroad of military data than by the domestic disclosure of such data. Technical data that is relatively harmless and even socially valuable when available domestically may, when sent abroad, pose unique threats to national security. It would hardly serve First Amendment values to compel the government to purge the public libraries of every scrap of data whose export abroad it deemed for security reasons necessary to prohibit.

United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989).

The Court also notes, as set forth above, that the ITAR provides a method through the commodity jurisdiction request process for determining whether information is subject to its export controls. See 22 C.F.R. § 120.4 (describing process). The regulations include a ten day deadline for providing a preliminary response, as well as a provision for requesting expedited processing. 22 C.F.R. § 120.4(e) (setting deadlines). Further, via Presidential directive, the DDTC is required to “complete the review and adjudication of license applications within 60 days of receipt.” 74 Fed. Reg. 63497 (December 3, 2009). Plaintiffs thus have available a process for determining whether the speech they wish to engage in is subject to the licensing scheme of the ITAR regulations.

Accordingly, the Court concludes Plaintiffs have not shown a substantial likelihood of success on the merits of their claim under the First Amendment.

D. Second Amendment

Plaintiffs also argue the ITAR regulatory scheme violates their rights under the Second Amendment. Defendants contend Plaintiffs cannot succeed on this claim, both because they lack standing to raise it, and because the claim fails on the merits. As standing is jurisdictional, the Court will turn to that issue first.

a. Standing

Article III of the Constitution limits the jurisdiction of federal courts to cases and controversies. *United States Parole Comm'n v. Geraghty*, 445 U.S. 388, 395 (1980). “One element of the case-or-controversy requirement is that [plaintiffs], based on their complaint, must establish that they have standing to sue.” *Raines v. Byrd*, 521 U.S. 811, 818 (1997). This requirement, like other jurisdictional requirements, is not subject to waiver and demands strict compliance. *Raines*, 521 U.S. at 819; *Lewis v. Casey*, 518 U.S. 343, 349 n.1 (1996). To meet the standing requirement a plaintiff must show (1) she has suffered an “injury in fact” that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Env'tl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); *Consol. Cos., Inc. v. Union Pacific R.R. Co.*, 499 F.3d 382, 385 (5th Cir. 2007); *Fla. Dep't of Ins. v. Chase Bank of Tex. Nat'l Ass'n*, 274 F.3d 924, 929 (5th Cir. 2001) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). “The party invoking federal jurisdiction bears the burden of establishing these elements.” *Lujan*, 504 U.S. at 561.

Defendants correctly point out Defense Distributed is in full possession of the computer files at issue and thus cannot argue it is being prevented from exercising its rights under the Second Amendment.⁴ Plaintiffs maintain Defense Distributed nonetheless has standing because it is “entitled to assert the Second Amendment rights of [its] customers and website visitors.” (Plf. Brf. at 27). A litigant is generally limited to asserting standing only on behalf of himself. See *Kowalski v. Tesmer*, 543 U.S. 125, 129 (2004) (a party “generally must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties”). The

⁴ No party addressed whether a corporation such as Defense Distributed itself possesses Second Amendment rights.

Supreme Court has recognized a limited exception when the litigant seeking third-party standing has suffered an "injury in fact" giving him a "sufficiently concrete interest" in the outcome of the issue, the litigant has a "close" relationship with the third party on whose behalf the right is asserted and there is a "hindrance" to the third party's ability to protect his own interests. *Powers v. Ohio*, 499 U.S. 400, 411 (1991).

Plaintiffs argue they meet this test, asserting Defense Distributed acts as a "vendor" or in a like position by way of offering the computer files for download to visitors of its website. See *Carey v. Population Servs. Int'l*, 431 U.S. 678, 684 (1977) ("vendors and those in like positions . . . have been uniformly permitted to resist efforts at restricting their operations by acting as advocates for the rights of third parties who seek access to their market or function"); *Reliable Consultants, Inc. v. Earle*, 517 F.3d 738, 743 (5th Cir. 2008) (Supreme Court precedent holds providers of product have standing to attack ban on commercial transactions involving product). As an initial matter, it is not at all clear that distribution of information for free via the Internet constitutes a commercial transaction.⁵ Moreover, Plaintiffs do not explain how visitors to Defense Distributed's website are hindered in their ability to protect their own interests. In fact, the presence of SAF as a plaintiff suggests to the contrary. Thus, whether Defense Distributed has standing to assert a claim of a violation of the Second Amendment is a very close question.

Lack of standing by one plaintiff is not dispositive, however. See *Village of Arlington Heights v. Metro. Hous. Dev. Corp.*, 429 U.S. 252, 264 (1977) (court need not decide third-party standing question, "[f]or we have at least one individual plaintiff who has demonstrated standing to assert these rights as his own"). And SAF's standing presents a much less difficult question. It asserts it has standing, as an association, to assert the rights of its members. See *Warth v.*

⁵ Defense Distributed describes itself as organized and operated "for the purpose of defending the civil liberty of popular access to arms guaranteed by the United States Constitution" through "facilitating global access to" information related to 3D printing of firearms, and specifically "to publish and distribute, *at no cost to the public*, such information and knowledge on the Internet in promotion of the public interest." (Compl. ¶ 1) (emphasis added).

Seldin, 422 U.S. 490, 511 (1975) (“[e]ven in the absence of injury to itself, an association may have standing solely as the representative of its members”). Associational standing requires showing: (1) the association’s members have standing to sue in their own right; (2) the interests at issue are germane to the association’s purpose; and (3) the participation of individual members in the lawsuit is not required. *Ass’n of Am. Physicians & Surgeons, Inc. v. Tex. Med. Bd.*, 627 F.3d 547, 550-51 (5th Cir. 2010) (citing *Hunt v. Wash. St. Apple Adver. Comm’n*, 432 U.S. 333, 343 (1977)). “The first prong requires that at least one member of the association have standing to sue in his or her own right.” *National Rifle Ass’n of Am., Inc. v. Bureau of Alcohol, Tobacco, Firearms, & Explosives*, 700 F.3d 185, 191 (5th Cir. 2012).

Defendants limit their challenge to SAF’s standing solely to whether any of its members have standing to sue in their own right. Specifically, Defendants contend SAF has merely asserted a conjectural injury, by suggesting its members would access computer files in the future. In response, SAF has provided affidavit testimony from two of its members stating they would access the computer files at issue via the Defense Distributed website, study, learn from and share the files, but are unable to do so due to Defendants’ interpretation of the ITAR regulatory scheme. (Plf. Reply Exs. 3-4). This testimony satisfies the “injury in fact” portion of the standing inquiry.

Defendants further contend any injury is not fairly traceable to their conduct. They argue the ITAR does not prevent SAF members in the United States from acquiring the files directly from Defense Distributed. But this argument goes to the burden imposed on SAF members, which is a question aimed at the merits of the claim, not standing. *See Davis v. United States*, 131 S. Ct. 2419, 2434, n.10 (one must not “confus[e] weakness on the merits with absence of Article III standing”). In this case, the inability of SAF members to download the computer files at issue off the Internet is the injury in fact of the SAF members, and is clearly traceable to the conduct of Defendants. The Court therefore finds SAF has standing to assert a claim of a violation of the Second Amendment. *See Nat’l Rifle Ass’n*, 700 F.3d at 192 (NRA had standing, on behalf of its

members under 21, to bring suit challenging laws prohibiting federal firearms licensees from selling handguns to 18-to-20-year-olds); *Ezell v. City of Chicago*, 651 F.3d 684, 696 (7th Cir. 2011) (SAF and Illinois Rifle Association had associational standing to challenge city ordinances requiring one hour of firing range training as prerequisite to lawful gun ownership and prohibiting all firing ranges in city); *Mance v. Holder*, 2015 WL 567302, at *5 (N.D. Tex. Feb. 11, 2015) (non-profit organization dedicated to promoting Second Amendment rights had associational standing to bring action challenging federal regulatory regime as it relates to buying, selling, and transporting of handguns over state lines).

b. Merits

The Second Amendment provides: “A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.” U.S. Const. amend. II. The Supreme Court has recognized that the Second Amendment confers an individual right to keep and bear arms. *See District of Columbia v. Heller*, 554 U.S. 570, 595 (2008). The Fifth Circuit uses a two-step inquiry to address claims under the Second Amendment. The first step is to determine whether the challenged law impinges upon a right protected by the Second Amendment—that is, whether the law regulates conduct that falls within the scope of the Second Amendment’s guarantee. The second step is to determine whether to apply intermediate or strict scrutiny to the law, and then to determine whether the law survives the proper level of scrutiny. *Nat’l Rifle Ass’n*, 700 F.3d at 194.

In the first step, the court is to “look to whether the law harmonizes with the historical traditions associated with the Second Amendment guarantee.” *Id.* (citing *Heller*, 554 U.S. at 577-628). Defendants argue at some length that restriction by a sovereign of export of firearms and other weapons has a lengthy historical tradition. Plaintiffs do not contest otherwise. Rather, Plaintiffs contend the conduct regulated here impinges on the ability to manufacture one’s own

firearms, in this case, by way of 3D printing.

While the founding fathers did not have access to such technology,⁶ Plaintiffs maintain the ability to manufacture guns falls within the right to keep and bear arms protected by the Second Amendment. Plaintiffs suggest, at the origins of the United States, blacksmithing and forging would have provided citizens with the ability to create their own firearms, and thus bolster their ability to “keep and bear arms.” While Plaintiffs’ logic is appealing, Plaintiffs do not cite any authority for this proposition, nor has the Court located any. The Court further finds telling that in the Supreme Court’s exhaustive historical analysis set forth in *Heller*, the discussion of the meaning of “keep and bear arms” did not touch in any way on an individual’s right to manufacture or create those arms. The Court is thus reluctant to find the ITAR regulations constitute a burden on the core of the Second Amendment.

The Court will nonetheless presume a Second Amendment right is implicated and proceed with the second step of the inquiry, determining the appropriate level of scrutiny to apply. Plaintiffs assert strict scrutiny is proper here, relying on their contention that a core Second Amendment right is implicated. However, the appropriate level of scrutiny “depends on the nature of the conduct being regulated *and* the degree to which the challenged law burdens the right.” *Nat’l Rifle Ass’n*, 700 F.3d at 195 (emphasis added).

The burden imposed here falls well short of that generally at issue in Second Amendment cases. SAF members are not prevented from “possess[ing] and us[ing] a handgun to defend his or her home and family.” *Id.* at 195 (citations omitted). The Fifth Circuit’s decision in *National Rifle Association* is instructive. At issue was a regulatory scheme which prohibited federally licensed firearms dealers from selling handguns to persons under the age of twenty-one. The court reasoned that only intermediate scrutiny applied for three reasons: (1) an age qualification on

⁶ Nonetheless, “the Second Amendment extends, *prima facie*, to all instruments that constitute bearable arms, even those that were not in existence at the time of the founding.” *Heller*, 554 U.S. at 582.

commercial firearm sales was significantly different from a total prohibition on handgun possession; (2) the age restriction did not strike at the core of the Second Amendment by preventing persons aged eighteen to twenty from possessing and using handguns for home defense because it was not a historical outlier; and (3) the restriction only had temporary effect because the targeted group would eventually age out of the restriction's reach. *Id.* at 205–07. In this case, SAF members are not prohibited from manufacturing their own firearms, nor are they prohibited from keeping and bearing other firearms. Most strikingly, SAF members in the United States are not prohibited from acquiring the computer files at issue directly from Defense Distributed. The Court thus concludes only intermediate scrutiny is warranted here. *See also Nat'l Rifle Ass'n of Am., Inc. v. McCraw*, 719 F.3d 338, 347-48 (5th Cir. 2013), *cert. denied*, 134 S. Ct. 1365 (2014) (applying intermediate scrutiny to constitutional challenge to state statute prohibiting 18-20-year-olds from carrying handguns in public).

As reviewed above, the regulatory scheme of the AECA and ITAR survives an intermediate level of scrutiny, as it advances a legitimate governmental interest in a not unduly burdensome fashion. *See also McCraw*, 719 F.3d at 348 (statute limiting under 21-year-olds from carrying handguns in public advances important government objective of advancing public safety by curbing violent crime); *Nat'l Rifle Ass'n*, 700 F.3d at 209 (“The legitimate and compelling state interest in protecting the community from crime cannot be doubted.”). Accordingly, the Court finds Plaintiffs have not shown a substantial likelihood of success on the merits.

E. Fifth Amendment

Plaintiffs finally argue the prior restraint scheme of the ITAR is void for vagueness and thus in violation of their right to due process. “It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined.” *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). The Fifth Amendment prohibits the enforcement of vague criminal laws, but

the threshold for declaring a law void for vagueness is high. “The strong presumptive validity that attaches to an Act of Congress has led this Court to hold many times that statutes are not automatically invalidated as vague simply because difficulty is found in determining whether certain marginal offenses fall within their language.” *United States v. Nat’l Dairy Prods. Corp.*, 372 U.S. 29, 32 (1963). Rather, it is sufficient if a statute sets out an “ascertainable standard.” *United States v. L. Cohen Grocery Co.*, 255 U.S. 81, 89 (1921). A statute is thus void for vagueness only if it wholly “fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.” *United States v. Williams*, 553 U.S. 285, 304 (2008).

Plaintiffs here assert broadly that ITAR is unconstitutionally vague because “persons of ordinary intelligence” must guess as to whether their speech would fall under its auspices. As an initial matter, the Court notes at least two circuits have rejected due process challenges to the AECA and ITAR, and upheld criminal convictions for its violation. *See Zhen Zhou Wu*, 711 F.3d at 13 (rejecting defendants’ argument “that this carefully crafted regulatory scheme—which has remained in place for more than a quarter century—is unconstitutionally vague” as applied to them); *United States v. Hsu*, 364 F.3d 192, 198 (4th Cir. 2004) (holding the AECA and its implementing regulations not unconstitutionally vague as applied to defendants). Plaintiffs neither acknowledge those decisions nor explain how their rationale is inapplicable to their situation.

The Supreme Court has recently noted its precedent generally limits such challenges to “statutes that tied criminal culpability” to conduct which required “wholly subjective judgments without statutory definitions, narrowing context, or settled legal meanings.” *Humanitarian Law Project*, 561 U.S. at 20 (quoting *Williams*, 553 U.S. at 306). Plaintiffs’ challenge here is additionally hampered because they have not made precisely clear which portion of the ITAR language they believe is unconstitutionally vague.

To the degree Plaintiffs contend “defense articles” is vague, as Defendants point out, the

term “defense articles” is specifically defined to include items on the Munitions List, which contains twenty-one categories of governed articles, as well as information “which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles” which additionally “includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.” See 22 C.F.R. §§ 120.6 (defining “defense articles”), 120.10 (a) (defining technical data) & 121.1 (Munitions List). Although lengthy, the cited regulations do not themselves include subjective terms, but rather identify items with significant specificity. For example, the first category “Firearms, Close Assault Weapons and Combat Shotguns” includes eight subcategories such as “Nonautomatic and semi-automatic firearms to caliber .50 inclusive (12.7 mm),” as well as six interpretations of the terms. 22 C.F.R. § 121.1. The Court has little trouble finding these provisions survive a vagueness challenge.

The term “export” is also defined in the ITAR, although at lesser length. At issue here, “export” is defined to include “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad.” 22 C.F.R. § 120.17(a)(4). Plaintiffs here admit they wish to post on the Internet, for free download, files which include directions for the 3D printing of firearms. Persons of ordinary intelligence are clearly put on notice by the language of the regulations that such a posting would fall within the definition of export.

Accordingly, the Court concludes Plaintiffs have not shown a likelihood of success on the merits of their claim under the Fifth Amendment.

IV. CONCLUSION

Plaintiffs' Motion for Preliminary Injunction (Clerk's Dkt. #7) is hereby **DENIED**.

SIGNED on August 4, 2015.

A handwritten signature in black ink, appearing to read "R. Pitman", with a horizontal line extending to the right.

ROBERT L. PITMAN
UNITED STATES DISTRICT JUDGE

SEN. JOHNSON, MISSOURI, CHAIRMAN

JOHN MCCAIN, ARIZONA
BOB PORTMAN, OHIO
RAND PAUL, KENTUCKY
JAMES LANKFORD, OKLAHOMA
MICHAEL B. ENO, WYOMING
KELLY AYOTTE, NEW HAMPSHIRE
JON HIRST, IOWA
SEN. LARSEN, MONTANATHOMAS R. CARPER, DELAWARE
CLARKE MCGASKILL, MISSISSIPPI
JOHN HESTER, MONTANA
TAMMY BALDWIN, WISCONSIN
ROD HUTTENLOPP, NORTH CAROLINA
CLAY A. BUCKNER, NEW JERSEY
GARY C. PETERS, MICHIGAN

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250KEITH B. ANDERSON, STAFF DIRECTOR
GABRIELLE A. RATON, SENIORITY STAFF DIRECTOR

July 16, 2015

The Honorable John Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, D.C. 20520

Dear Secretary Kerry:

We write to express concern about State Department's recently-proposed changes to the International Traffic in Arms Regulations (ITAR). If finalized, the proposal could significantly hinder the First and Second Amendment rights of millions of law-abiding citizens. In light of these serious constitutional concerns, we ask for your assistance in better understanding the legal rationale and the basis for the proposed ITAR changes.

As you are aware, the Arms Export Control Act (AECA) charges the President with the task of regulating international arms trafficking "in furtherance of world peace and the security and foreign policy of the United States."¹ The State Department has developed the ITAR regulatory framework to fulfill the statutory mission outlined in the AECA.² ITAR regulations are designed to regulate the transmission or sale of military equipment that has the "capacity for substantial military utility or capability such as tanks, high explosives, naval vessels, attack helicopters," and more.³ The current ITAR framework regulates the dissemination of technical information referring to these weapons of war including information that is distributed in the "public domain."⁴

It appears that the proposed ITAR changes seek to regulate activities that extend beyond the original intent of the AECA to cover items that previously were not subject to ITAR regulation. The Department's proposed rule expands "public domain" regulations to include published information relating to "technical data" of "defense articles."⁵ The proposal expands the definition of "defense article" to include items such as firearms and accompanying software

¹ 22 U.S.C. § 2778(a)(1).

² *The International Traffic in Arms Regulations (ITAR)*, Directorate of Defense Trade Controls, https://www.pmdtc.state.gov/regulations_laws/itar.html, (last visited July 8, 2015).

³ *What is ITAR?*, Government Relations LLC, <https://gov-relations.com/itar/> (last visited July 8, 2015).

⁴ 79 Fed. Reg. 27185 (May 13, 2014) http://www.ecfr.gov/cgi-bin/text-idx?SID=2fc28ab4acb809959171d797493f5346&mc=true&node=se22.1.120_110&rgn=div8.

⁵ International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions, 80 Fed. Reg. 31525 at 31534-35 (proposed June 3, 2015) (to be codified at 22 C.F.R. pt. 120) <http://www.gpo.gov/fdsys/pkg/FR-2015-06-03/pdf/2015-12844.pdf>.

The Honorable John Kerry

July 16, 2015

Page 2

or “technical data.”⁶ Under the proposal, “technical data” may even encompass information relating to repair and maintenance of “defense articles.”⁷ Further, under the proposal, people who intend to discuss “technical data” about firearms, firearm-related 3D printing, and explosives in the “public domain” may be forced to seek “proper authorization” from government authorities such as the Directorate of Defense Trade Controls before engaging in such discussions.⁸ In application and effect, this governmental scheme appears to act as a prior restraint. As such, not only does the regulation arguably impede upon a person’s ability to exercise their fundamental rights under the First Amendment but the Second Amendment, too.

While there are certainly benefits in preventing the exportation of sensitive information related to high-powered weaponry, the proposed regulation could extend to citizens engaging in legal activities, potentially exposing them to fines and criminal prosecutions. Millions of firearm owners and 3D printer users who use the Internet to discuss their hobbies could unintentionally violate the law if these changes to ITAR move forward.

Because the proposal grants the State Department the power to classify what is and what is not in the “public domain” for “defense articles” under ITAR, the Department will apparently have unilateral authority to require citizens to seek preapproval for what had previously been free speech.⁹ Given the proposal’s nexus to firearms, a number of Second Amendment and Constitutional rights organizations have expressed concern over the chilling effects that this regulation may have on free speech and the right to bear arms.¹⁰ When asked about these constitutional implications, the State Department has been unable to adequately clarify what specific activities would be subject to preapproval under the proposal.¹¹ So far, during the public

⁶ *Id.* at 31534, § 120.6 (defense article means any item, software, or technical data designated in § 121.1 of this subchapter).

⁷ *Id.*, § 120.10 ((information required for the development (see § 120.47) (including design, modification, and integration design), production (see § 120.48) (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article)).

⁸ *Id.* at 31535, note 1 to § 120.11 ((section 127.1(a)(6) of this subchapter prohibits, without written authorization from the Directorate of Defense Trade Controls, U.S. and foreign persons from exporting, reexporting, retransferring, or otherwise making available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in paragraph (b) of this section.))

⁹ *Id.*

¹⁰ See *Stop Obama’s Planned Gag Order on Firearm-Related Speech*, NRA Institute for Legislative Action (June 5, 2015) <https://www.nraila.org/articles/20150605/stop-obamas-planned-gag-order-on-firearm-related-speech>; Charles C.W. Cooke, *The State Department’s Dangerous New Proposal to Regulate Gun Enthusiasts’ Internet Speech*, Nat’l Review (June 9, 2015) <http://www.nationalreview.com/article/419489/obama-administration-supports-free-internet-except-when-it-comes-gun-enthusiasts>.

¹¹ Press Release, U.S. Dept. of State, Daily Press Briefing (June 10, 2015) (when asked if the proposed regulations would restrict discussions regarding firearms, the Department spokesperson stated “[w]ell, I go back to the – also the point that general descriptions – that is general, not technical and detailed ones – general descriptions or public discussions and imagery of defense articles would – have never been subject to these regulations and wouldn’t.” The spokesperson does not address the fact that videos or information on firearm repair and maintenance could be considered “technical” under the proposed changes) <http://www.state.gov/r/pa/prs/dpb/2015/06/243337.htm>.

The Honorable John Kerry
July 16, 2015
Page 3

comment period, over six thousand comments have been submitted by citizens, with the overwhelming majority opposing these proposed changes.¹²

As currently constructed, the State Department's proposal seems to conflict with constitutional principles. In order to understand the State Department's authority and rationale behind the proposed changes, I ask that you please provide the following information and materials:

1. Please provide an explanation of the State Department's legal authority for the proposed ITAR changes.
2. Did State Department officials communicate with the White House or other Executive Branch agencies about the drafting of the proposed changes under ITAR? Please provide all communications between or among State Department employees and employees of the White House or any other Executive Branch agency or department referring or relating to the promulgation of the proposed ITAR regulation.
3. There is tremendous uncertainty surrounding the Department's proposal. Could the following scenarios constitute a discussion of "technical data" or "defense articles" in the "public domain" and thereby require "proper authorization" from the government before engaging in such discussions? Please explain:
 - a. An American citizen posts a video to YouTube showing other gun owners how to disassemble and clean an AR-15 rifle;
 - b. A Wisconsin or Iowa hunter creates a website dedicated to hunting birds (e.g. ducks, pheasants, etc.) On the website, the user posts a diagram on a forum detailing the individual parts and pieces of a shotgun commonly used to hunt birds. The same user also posts on the website videos explaining how to properly shoot a flying duck without ruining the meat on the bird. The website is read and commented upon by many Canadian bird hunters;
 - c. An American user comments on a foreign gun manufacturer's Internet forum on the technical specifications of a handgun they are considering purchasing from the foreign manufacturer; and
 - d. An American owner of a World War II-era Browning Automatic Rifle e-mails an instructional guide to a fellow World War II-era gun enthusiast in Germany on how to use a 3D printer to make a firing pin that will enable the operation of the weapon.

¹² *International Traffic in Arms: Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions*, Regulations.gov, <http://www.regulations.gov/#!documentDetail;D=DOS-2015-0023-0483> (last visited July 8, 2015).

The Honorable John Kerry

July 16, 2015

Page 4

4. The State Department has publicly stated that only "technical" and "detailed" descriptions of "defense articles" would be subject to the new proposed ITAR regulations while "general descriptions" would not. Please explain when and how an online discussion regarding a firearm would shift from being "general" to "technical" under the proposed ITAR changes.

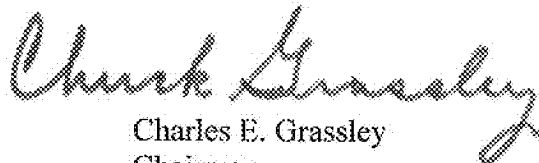
Please provide this material as soon as possible but no later than 5:00 p.m. on July 30, 2015.

If you have any questions please contact Kyle Brosnan or Scott Wittmann of Chairman Johnson's Staff at 202-224-4751 and Josh Flynn-Brown of Chairman Grassley's Staff at 202-224-5225. Thank you for your attention to this important matter.

Sincerely,



Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs



Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary



United States Department of State

Washington, D.C. 20520

AUG 11 2015

Dear Mr. Chairman:

Thank you for your July 16 letter regarding the Department of State's June 3, 2015, Federal Register Notice (80 FR 31525) proposing changes to the International Traffic in Arms Regulations (ITAR). We would like to take the opportunity to clarify the controls in place for the export of defense articles, including technical data, and defense services subject to the ITAR, and how this proposed rule will affect those controls. The Department has received a significant number of comments from the public offering their views on this proposed rule, and we will carefully review the comments and, where appropriate, incorporate the suggested revisions prior to issuing a final rule. Detailed answers to the specific questions in your letter are included in the addendum to this letter.

The Arms Export Control Act (AECA) authorizes the President "in furtherance of world peace and the security and foreign policy of the United States...to control the import and the export of defense articles and defense services...The President is authorized to designate those items which shall be considered as defense articles and defense services...*and to promulgate regulations for the import and export of such articles and services.* The items so designated shall constitute the United States Munitions List."

The statutory authority of the President to "promulgate regulations for the import and export of such articles and services" has been delegated to the Secretary of State by Executive Order 13637. The ITAR implements the AECA and is the regulatory structure for controlling the export of defense articles and defense services.

The Honorable
Ron Johnson, Chairman,
Committee on Homeland Security,
and Governmental Affairs,
United States Senate.

-2-

The items designated as defense articles constitute the United States Munitions List (USML), which ranges from the firearms addressed in your letter to missiles, stealth aircraft, submarines, and chemical and biological agents, and can be found in section 121.1 of the ITAR. All defense articles, including all directly related technical data and software, and defense services are subject to the controls outlined in the ITAR.

The ITAR helps promote U.S. national security and foreign policy interests by controlling the export of defense articles and defense services to foreign persons. The ITAR does not impose restrictions on person-to-person communications between U.S. persons when such communications take place within the United States. Currently, the ITAR regulates exports of all firearms except long barreled shotguns. In fact, since the introduction of the ITAR in 1957, firearms have been included on USML and thereby controlled for export under the ITAR, as is all directly related technical data and, since 1984, software directly related to these firearms.

The ITAR defines technical data as information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. However, many types of information are not considered to be technical data, including general system descriptions, information concerning general scientific, mathematical or engineering principles commonly taught in schools, or information appropriately placed into the public domain. Public domain information, as defined in the ITAR, is information that is published and generally accessible or available to the public and includes information available for sale through newsstands and bookstores, information available at libraries open to the public, and information resulting from certain fundamental research. The ITAR establishes mechanisms for an authorized U.S. government department or agency to approve the public release of technical data, which can include information on servicing F-16s or design information related to missile systems.

-3-

The release mechanisms currently found in the ITAR and the proposed revisions to the definitions of public domain and technical data were drafted in such a way that U.S. citizens' rights secured by the Constitution are protected.

The ITAR requires U.S. government approval prior to effectuating an export of defense articles and U.S. government authorization prior to placing ITAR controlled technical data into the public domain. This is because such activity is virtually certain to result in exports, as the technical data is made available to and may be freely accessed by foreign persons.

The changes proposed in the Department's June 3, 2015, Federal Register Notice (80 FR 31525) are primarily updates and clarifications of the current ITAR controls. Such updates and clarifications are necessary, as the controls on technical data have been largely unmodified since 1984. Many of these changes are designed to bring this control language more in line with current technology and mechanisms for exporting, including sending email. The changes update and clarify the controls within the ITAR, including explicitly describing how electronic information is controlled. One major change includes a provision that relates to the handling of encrypted internet traffic.

The proposed change to the definition of public domain is intended to simplify, update, and introduce greater versatility into the definition, as well as clarify how to obtain authorization prior to making ITAR-controlled technical data available to the public. The updated definition also proposes that individuals who obtain information from publically available sources do not need to confirm that the information was released lawfully. The public may republish or otherwise export such information without needing to confirm the nature of its release. However, individuals who know of an unlawful public release and seek to take advantage to export technical data do so unlawfully.

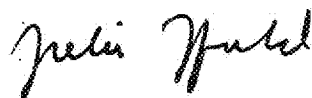
Individuals who are generally discussing defense articles, whether firearms or missiles, do not require an ITAR authorization. Individuals involved in technical discussions about such items using information properly in the public domain do not require an ITAR authorization. Even U.S. persons in the U.S. describing detailed technical data to other U.S. persons regarding the design,

-4-

development, production, or manufacture of a defense article do not require an authorization. An ITAR authorization or other release approval, as outlined in the ITAR, is only required prior to the export or public release of technical data, such as when a U.S. person provides technical details on a defense article to a foreign person, or when technical data is posted to a public website and thereby made available to a foreign person.

Please be assured that the Department will review and respond to the public comments received on the proposed rule as part of the rule making process. We appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs

Enclosure:

Addendum.



United States Department of State

Washington, D.C. 20520

AUG 11 2015

Dear Mr. Chairman:

Thank you for your July 16 letter regarding the Department of State's June 3, 2015, Federal Register Notice (80 FR 31525) proposing changes to the International Traffic in Arms Regulations (ITAR). We would like to take the opportunity to clarify the controls in place for the export of defense articles, including technical data, and defense services subject to the ITAR, and how this proposed rule will affect those controls. The Department has received a significant number of comments from the public offering their views on this proposed rule, and we will carefully review the comments and, where appropriate, incorporate the suggested revisions prior to issuing a final rule. Detailed answers to the specific questions in your letter are included in the addendum to this letter.

The Arms Export Control Act (AECA) authorizes the President "in furtherance of world peace and the security and foreign policy of the United States...to control the import and the export of defense articles and defense services...The President is authorized to designate those items which shall be considered as defense articles and defense services...*and to promulgate regulations for the import and export of such articles and services.* The items so designated shall constitute the United States Munitions List."

The statutory authority of the President to "promulgate regulations for the import and export of such articles and services" has been delegated to the Secretary of State by Executive Order 13637. The ITAR implements the AECA and is the regulatory structure for controlling the export of defense articles and defense services.

The Honorable
Charles E. Grassley, Chairman,
Committee on the Judiciary,
United States Senate.

-2-

The items designated as defense articles constitute the United States Munitions List (USML), which ranges from the firearms addressed in your letter to missiles, stealth aircraft, submarines, and chemical and biological agents, and can be found in section 121.1 of the ITAR. All defense articles, including all directly related technical data and software, and defense services are subject to the controls outlined in the ITAR.

The ITAR helps promote U.S. national security and foreign policy interests by controlling the export of defense articles and defense services to foreign persons. The ITAR does not impose restrictions on person-to-person communications between U.S. persons when such communications take place within the United States. Currently, the ITAR regulates exports of all firearms except long barreled shotguns. In fact, since the introduction of the ITAR in 1957, firearms have been included on USML and thereby controlled for export under the ITAR, as is all directly related technical data and, since 1984, software directly related to these firearms.

The ITAR defines technical data as information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. However, many types of information are not considered to be technical data, including general system descriptions, information concerning general scientific, mathematical or engineering principles commonly taught in schools, or information appropriately placed into the public domain. Public domain information, as defined in the ITAR, is information that is published and generally accessible or available to the public and includes information available for sale through newsstands and bookstores, information available at libraries open to the public, and information resulting from certain fundamental research. The ITAR establishes mechanisms for an authorized U.S. government department or agency to approve the public release of technical data, which can include information on servicing F-16s or design information related to missile systems.

-3-

The release mechanisms currently found in the ITAR and the proposed revisions to the definitions of public domain and technical data were drafted in such a way that U.S. citizens' rights secured by the Constitution are protected.

The ITAR requires U.S. government approval prior to effectuating an export of defense articles and U.S. government authorization prior to placing ITAR controlled technical data into the public domain. This is because such activity is virtually certain to result in exports, as the technical data is made available to and may be freely accessed by foreign persons.

The changes proposed in the Department's June 3, 2015, Federal Register Notice (80 FR 31525) are primarily updates and clarifications of the current ITAR controls. Such updates and clarifications are necessary, as the controls on technical data have been largely unmodified since 1984. Many of these changes are designed to bring this control language more in line with current technology and mechanisms for exporting, including sending email. The changes update and clarify the controls within the ITAR, including explicitly describing how electronic information is controlled. One major change includes a provision that relates to the handling of encrypted internet traffic.

The proposed change to the definition of public domain is intended to simplify, update, and introduce greater versatility into the definition, as well as clarify how to obtain authorization prior to making ITAR-controlled technical data available to the public. The updated definition also proposes that individuals who obtain information from publically available sources do not need to confirm that the information was released lawfully. The public may republish or otherwise export such information without needing to confirm the nature of its release. However, individuals who know of an unlawful public release and seek to take advantage to export technical data do so unlawfully.

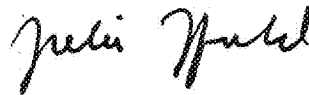
Individuals who are generally discussing defense articles, whether firearms or missiles, do not require an ITAR authorization. Individuals involved in technical discussions about such items using information properly in the public domain do not require an ITAR authorization. Even U.S. persons in the U.S. describing detailed technical data to other U.S. persons regarding the design,

-4-

development, production, or manufacture of a defense article do not require an authorization. An ITAR authorization or other release approval, as outlined in the ITAR, is only required prior to the export or public release of technical data, such as when a U.S. person provides technical details on a defense article to a foreign person, or when technical data is posted to a public website and thereby made available to a foreign person.

Please be assured that the Department will review and respond to the public comments received on the proposed rule as part of the rule making process. We appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs

Enclosure:

Addendum.

Addendum

1. The authority for the International Traffic in Arms Regulations (ITAR) flows from the Arms Export Control Act (AECA), Section 38(a)(1), which authorizes the President “in furtherance of world peace and the security and foreign policy of the United States...to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.”

The statutory authority of the President to “promulgate regulations for the import and export of such articles and services” has been delegated to the Secretary of State by Executive Order 13637, which provides in section 1(n) that “[t]hose [authorities] under section 38 of the Act (22 U.S.C. 2778) [are delegated to] the Secretary of State, except as otherwise provided in this subsection. Designations, including changes in designations, by the Secretary of State of items or categories of items that shall be considered as defense articles and defense services subject to export control under section 38 (22 U.S.C. 2778) shall have the concurrence of the Secretary of Defense.”

Prior to the passage of the AECA in 1976, the ITAR was similarly authorized under the Mutual Security Act of 1954 (MSA) and the relevant statutory authority was delegated from the President to the Secretary of State by Executive Orders 10575, 10893, and 10973. Like the AECA, the MSA authorized the President “to control, in furtherance of world peace and the security and foreign policy of the United States, the export and import of arms, ammunition, and implements of war, including technical data relating thereto...”

2. The proposed changes to the ITAR were drafted in close coordination with the Departments of Commerce and Defense and were subjected to a thorough

interagency vetting process, with active participation and clearance by the Department of Commerce, Department of Defense, Department of Justice, and Department of Homeland Security, as well as other offices within the Department of State. Following interagency agreement to publish the proposed rules for public comment, the proposed rules were officially coordinated and cleared by the Office of Information and Regulatory Affairs in the Office of Management and Budget at the White House.

3. Below, please find the analysis of each of the four scenarios that you posit in your letter, applying the changes as proposed in the Department's June 3, 2015, Federal Register Notice (80 FR 31525). As these are proposed changes for which the Department is soliciting public comments, please note that the Department may modify the proposed changes based on the public comments received.

- a. Information for disassembling and cleaning an AR-15 rifle is and has been in the public domain for many years and therefore would not require an authorization. Even if such information had originally been made publically available without appropriate authorization, the posting of such information to the internet by an unknowing second party in the form of a YouTube video would not require an authorization. As detailed in the proposed regulations at Note 2 to § 120.11, further dissemination of information that was made publically available by another person is not a violation of the ITAR, unless the subsequent dissemination is done with knowledge that the original placement in the public domain was done without authorization.
- b. A diagram of the parts and pieces of a shotgun would most likely not constitute technical data, nor would information on how to aim or fire a shotgun. This is because most shotguns are not defense articles, as they are not listed in the USML at § 121.1 of the ITAR. USML Category I(d) identifies combat shotguns, including all shotguns with a barrel length less than 18 inches. All other shotguns are controlled for export by the Department of Commerce under Export Control Classification Number (ECCN) 0A984 in the Commerce Control List (CCL) in the Export Administration Regulations (EAR). As detailed in the proposed

regulations at Note 3 to paragraph (a) of § 120.46, information that is for shotguns subject to the EAR, including information common to both shotguns subject to the EAR and to the ITAR, is information subject to the EAR. If the firearm were subject to the ITAR, then the fact pattern to determining whether the information is technical data and the activity controlled is outlined within this letter.

- c. Comments on the technical specification of a firearm would not usually be technical data or require an authorization. Technical specifications are not necessarily technical data. Technical data is, per the proposed § 120.10(a), information required for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article. While technical specifications are normally used to describe the attributes or performance of a defense article, they often do not constitute information on how or why the defense article was developed or produced and do not always provide any information on how to operate, install, maintain, repair, overhaul, or refurbish it. General instructional guides on how to use 3D printers are not controlled technical data and do not require an authorization, as 3D printers are not subject to the ITAR. Specific data, such as a CAD file that directly results in the printing or manufacturing of a defense article would, however, be technical data, unless it were released pursuant to a relevant part of section 120.11 of the ITAR.

4. Regarding your final request, to explain when and how an online discussion regarding a firearm would shift from being “general” to “technical” under the proposed ITAR changes, the Department notes that such discussions take many forms and that the below answer is not an exhaustive explanation of when online discussions may reveal technical data. Unclassified technical data is information required for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article, as described in ITAR § 120.10(a). However, as provided in ITAR § 120.6(b), information in the public domain, including information resulting from certain fundamental research or published in patents, or general scientific, mathematical, or engineering principles commonly taught in schools is excluded, as are general system descriptions and

information on its basic function or purpose of an item, per ITAR § 120.10(b). Information on how to perform custom modifications to a commercially available firearm that provide additional functionality or discussions on the development or production of a new firearm, such as for creation of CAD files to 3D print a firearm part or component, could constitute technical data, depending on whether the firearm is on the USML and the nature of the information being discussed (e.g., is it properly in the public domain). As such, while very detailed technical discussions amongst do-it-yourself gun hobbyists may cross into technical data, it is unlikely that discussions by the interested American public of generally commercially available firearms would rise to the level of technical data. Even if they did, such discussions between U.S. persons would not require authorization from the Department of State.



United States Department of State

Washington, D.C. 20520

JUL 21 2015

Dear Mr. Chairman:

Thank you for your letter of July 16 regarding the Department of State's June 3, 2015 Federal Register Notice proposing changes to the International Traffic in Arms Regulations. The Department is still compiling the necessary information to respond to your request. We will be in contact soon with responsive information.

We apologize for the delay, and appreciate your interest in this important matter. Please do not hesitate to contact us with any questions.

Sincerely,

A handwritten signature in cursive script that reads "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs

The Honorable

Ron Johnson, Chairman,

Committee on Homeland Security and Governmental Affairs,
United States Senate.



United States Department of State

Washington, D.C. 20520

JUL 21 2015

Dear Mr. Chairman:

Thank you for your letter of July 16 regarding the Department of State's June 3, 2015 Federal Register Notice proposing changes to the International Traffic in Arms Regulations. The Department is still compiling the necessary information to respond to your request. We will be in contact soon with responsive information.

We apologize for the delay, and appreciate your interest in this important matter. Please do not hesitate to contact us with any questions.

Sincerely,

A handwritten signature in cursive script that reads "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs

The Honorable
Charles E. Grassley, Chairman,
Committee on the Judiciary,
United States Senate.



NATIONAL SHOOTING SPORTS FOUNDATION, INC.

11 Mile Hill Road • Newtown, CT 06470-2359 • Tel (203) 426-1320 • Fax (203) 426-7182 • www.nssf.org

LAWRENCE G. KEANE
SENIOR VICE PRESIDENT
& GENERAL COUNSEL

September 28, 2015

President Barack Obama
The White House
Washington, D.C. 20050

Dear Mr. President,

On behalf of the National Shooting Sports Foundation (NSSF), the trade association for America's firearms, ammunition, hunting and shooting sports industry, I would like to congratulate you on the significant progress your Administration has made toward its Export Control Reform (ECR) initiative goals. Your goal of reforming America's export control to "build higher fences around fewer things" will help ensure that U.S. companies can compete in today's global economy, while improving our national security.

The NSSF is proud of its working relationship with your Administration, including the departments of Commerce and State. Both the Directorate of Defense Trade Controls (DDTC) and Bureau of Industry and Security (BIS) participate in our annual Firearms Industry Import/Export Conference. We have actively supported the important steps taken so far toward ECR and hope to see the initiative reach its full goals and modernize the Cold War-era export control regime before the end of your Administration. We continue to educate members of Congress on the importance of the ECR to the entire business community.

As you know, the interagency task force has been actively reviewing the United States Munitions List (USML) and the BIS Commerce Control List (CCL) so that the two lists may be rationalized and dual use items for the commercial market currently on the USML, be placed on the CCL where they can be controlled by the appropriate entity, while ensuring proposed exports will still be reviewed by the interagency community. The interagency review of the controls list and the stakeholder agreements have been complete for USML Categories I-III (sporting firearms, ammunition, and hunting rifles over .50 caliber) for more than 3 years. These are the only remaining categories yet to be published that have completed the list-related reforms in Phases I and II of the initiative. While other industries are beginning to realize the economic benefits of ECR, the firearms, ammunition, hunting and shooting sports industry remains on the sidelines awaiting the publication of the dual proposed rules to move our commercial and sporting products to BIS from DDTC.

As your second term continues, we urge you to move forward with ongoing export control reform efforts in a way that will help meet the dual goals of strengthening national

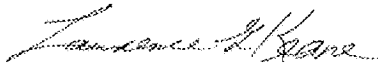
President Barack Obama

September 28, 2015

Page 2 of 2

security and boosting the U.S. economy. By implementing reforms including expanding the BIS's existing responsibility for the export licensing of sporting firearms, ammunition and related products to include items currently on Categories I-III, a more streamlined, efficient and transparent system is within reach. Tackling the archaic and inefficient export control system and making it work for the world we face today will be a major accomplishment when the process is complete. The NSSF looks forward to a constructive ongoing dialogue with your administration on your Export Control Reform Initiative and other issues affecting our industry.

Sincerely,

A handwritten signature in dark ink, appearing to read "Lawrence G. Keane", with a stylized flourish at the end.

Lawrence G. Keane

CC: Chairman Bob P. Corker, Senate Foreign Relations Committee
Ranking Member Ben Cardin, Senate Foreign Relations Committee
Chairman John Thune, Senate Commerce, Science & Transportation Committee
Ranking Member Bill Nelson, Senate Commerce, Science & Transportation Committee
Chairman Ed R. Royce, House Foreign Affairs Committee
Ranking Member Eliot Engel, House Foreign Affairs Committee
Chairman Fred S. Upton, House Energy and Commerce Committee
Ranking Member Frank Pallone, House Energy and Commerce Committee

BOB CORKER
TENNESSEE
<http://www.corker.senate.gov/>

420 Dirksen Senate Office Building
Washington, DC 20510
(202) 224-3044
Fax: (202) 228-0806

United States Senate

October 5, 2015

COMMITTEES:
BANKING, HOUSING,
AND URBAN AFFAIRS
BUDGET
FOREIGN RELATIONS
SPECIAL COMMITTEE ON AGING

The Honorable John F. Kerry
Secretary of State
United States Department of State
Washington, DC 20520

Dear Secretary Kerry,

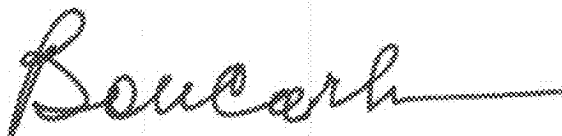
I write to you today to express my support for the Export Control Reform (ECR) Initiative. Significant progress has been made in advancing ECR. However, I ask that you work to expeditiously complete the review of the remaining categories of the U.S. Munitions List (USML) and publish for public comment the proposed rules to move eligible dual use items to the Commerce Control List (CCL).

In particular, I understand the interagency review of Categories I-III was completed some time ago and that the proposed rules have been drafted and vetted through the interagency task force, but have yet to be published for public comment. Given this advanced stage in the process, I ask that you inform me as to when the proposed rules for these categories will be published in the Federal Register for public comment.

Completing the reform and modernization of the United States export control regime is important to ensuring U.S. national security interests and helping U.S. companies remain competitive in the current global economy.

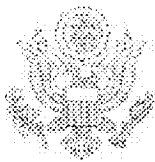
Thank you for your quick response to this inquiry.

Sincerely,



Bob Corker
United States Senator

CC: The Honorable Penny Pritzker, Secretary of Commerce



United States Department of State

Washington, D.C. 20520

FEB 05 2016

The Honorable
Bob Corker, Chairman
Committee on Foreign Relations
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Thank you for your October 5, 2015 letter expressing support for the President's Export Control Reform (ECR) Initiative. The Initiative is vital to U.S. national security and foreign policy interests. As you note, much progress has been made in advancing ECR to date, with 15 of the 21 U.S. Munitions List Categories revised. We have also made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).

The Department is focused on continuing this effort successfully. We are working toward reviewing the remaining USML categories, while beginning to re-review those that were last revised over two years ago. Additionally, our efforts include further work to clarify and harmonize certain definitions in the ITAR and the EAR, which was the subject of a recent proposed rule.

At this time, the Department's primary focus, as well as that of our interagency partners, is to finalize the significant number of proposed rule-makings currently in process, which include revisions to USML Categories XII and XIV. Nonetheless, the Department is committed to finalizing an initial review of the entire USML in 2016.

We appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in cursive script that reads "Julia Frifield".

Julia Frifield
Assistant Secretary
Legislative Affairs

BRADLEY BYRNE
1st District, Alabama

Serving BALDWIN, CLARKE,
ESCALONA, MOBILE, MONROE AND
WASHINGTON COUNTIES

HOUSE COMMITTEES:
ARMED SERVICES

EDUCATION AND THE WORKFORCE

RULES

Congress of the United States

House of Representatives

Washington, DC 20515

October 6, 2015

Secretary John Kerry
Department of State
2201 C Street, NW
Washington, D.C. 20520

Secretary Penny Pritzker
U.S. Department of Commerce
Room 5421
Fourteenth Street and Constitution Avenue, NW
Washington, DC 20230

Dear Secretary Kerry and Secretary Pritzker:

I write in support of the completion of President Barrack Obama's Export Control Reform Initiative (ECR). I urge you to work together to complete the implementation of this worthwhile initiative which is overwhelmingly supported by the business community.

Completing the reform and modernization of the United States export control system is imperative to ensuring that U.S. companies are competitive in the current global economy and to ensure that the nation meets the National Export Initiative (NEI) objective of doubling U.S. exports within five years. Currently, our export control system is enforced by multiple agencies with overlapping and redundant authorities. These agencies use separate IT systems and the export licensing process involves three independent licensing agencies which use two distinct control lists. This overly complicated and inefficient system burdens our economy and hinders U.S. exports. This system must be streamlined in order for U.S. companies to avoid redundancies that negatively impact American companies.

As you know, the interagency task force has been actively reviewing the United States Munitions List (USML) and the Bureau of Industry and Security (BIS) Commerce Control List (CCL) so that the two lists may be rationalized and dual use items for the commercial market currently on the USML, be placed on the CCL where they can be controlled by the appropriate entity, while keeping defense articles on the USML. The interagency review of the controls list and the stakeholder agreements have been complete for categories I-III (sporting firearms, ammunition, and hunting rifles over .50 caliber) for more than 3 years, and they are the only remaining categories yet to be published that have completed steps one and two. While other industries are beginning to see the benefits of ECR, the firearms and ammunition industry remains on the sidelines.

When can I expect to see the rule published in the federal record that will address categories I-III of the USML moving to the CCL? It is imperative for the competitiveness of US companies that

ECR is finally completed and the final categories are moved from the USML to the CCL and controlled by BIS. I appreciate your commitment to American exports and look forward to working with you to finish moving the final three categories to the CCL. Thank you for your attention to this important matter.

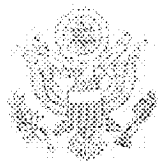
Sincerely,



Bradley Byrne

United States Department of State

Washington, D.C. 20520



FEB 05 2016

The Honorable
Bradley Byrne
House of Representatives
Washington, DC 20515

Dear Mr. Byrne:

Thank you for your October 6, 2015 letter expressing support for the President's Export Control Reform (ECR) Initiative. The Initiative is vital to U.S. national security and foreign policy interests. As you note, much progress has been made in advancing ECR to date, with 15 of the 21 U.S. Munitions List Categories revised. We have also made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).

The Department is focused on continuing this effort successfully. We are working toward reviewing the remaining USML categories, while beginning to re-review those that were last revised over two years ago. Additionally, our efforts include further work to clarify and harmonize certain definitions in the ITAR and the EAR, which was the subject of a recent proposed rule.

At this time, the Department's primary focus, as well as that of our interagency partners, is to finalize the significant number of proposed rule-makings currently in process, which include revisions to USML Categories XII and XIV. Nonetheless, the Department is committed to finalizing an initial review of the entire USML in 2016.

We appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in cursive script that reads "Julia Frisfield".

Julia Frisfield
Assistant Secretary
Legislative Affairs



Jay Timmons
President and CEO

October 7, 2015

President Barack Obama
The White House
Washington, DC 20050

Dear Mr. President,

The National Association of Manufacturers (NAM) has long supported the objectives of your Export Control Reform Initiative: to focus federal resources on the threats that matter most, to bring transparency and coherence to these regulations and to enhance the competitiveness of manufacturing and technology sectors in the United States. Accordingly, we appreciate the significant progress made by the Departments of State, Commerce and Defense toward the initiative's goals. We urge you, though, to quickly move forward with completing the review and reconciliation of the separate U.S. Munitions List (USML) and Commerce Control List (CCL).

The NAM is the nation's largest industrial trade association, representing small and large manufacturers in every industrial sector and in all 50 states. Our members drive America's global leadership in advanced technology and many play a critical role in protecting the security of the United States. Some are directly engaged in providing the technology and equipment that keep the U.S. military the best in the world. Others play a key support role, developing the advanced industrial technology, machinery and information systems necessary for our manufacturing, high-tech and services industries.

Since the initiative was launched in 2009, the Departments of State and Commerce have published dozens of proposed and final rules to update USML and CCL Categories and more properly classify technologies for control under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). In fact, proposed rules have been published for 16 of the 19 current USML Categories – leaving only USML Category I (Firearms), Category II (Guns) and Category III (Ammunition). The interagency review and stakeholder discussions on the proposals for USML Categories I, II and III have been completed, and we urge you to publishing those proposed rules in the Federal Register and to move toward finalizing the proposed changes.

While your Administration has made great strides in reconciling the separate control lists, we strongly urge you to complete that task as soon as possible. Although there are other much-needed management reforms that would further streamline licensing and system administration, completing the list review exercise should remain a priority.

We look forward to continuing to work with the White House as well as with the Departments of State and Commerce – and their partners – on this important initiative.

With all best wishes I remain,

Sincerely,

A handwritten signature in black ink, appearing to read 'Jay Timmons', is written over a printed name.

Jay Timmons

Leading Innovation. Creating Opportunity. Pursuing Progress.

ROY BLUNT
MISSOURI

VICE CHAIRMAN, SENATE REPUBLICAN CONFERENCE

280 Russell Senate Office Building
Washington, DC 20510-2808
(202) 224-5721

United States Senate
WASHINGTON, DC 20510

COMMITTEES
APPROPRIATIONS

COMMERCE, SCIENCE
AND TRANSPORTATION

CHAIRMAN, RULES AND
ADMINISTRATION

SELECT COMMITTEE
ON INTELLIGENCE

October 7, 2015

The Honorable John F. Kerry
Secretary of State
U.S. Department of State
Washington, DC 20520

The Honorable Penny Pritzker
Secretary of Commerce
U.S. Department of Commerce
Washington, DC 20230

Dear Secretary Kerry and Secretary Pritzker:

I write to express my support for the Export Control Reform Initiative (ECR), and to urge you to work to complete the implementation of this initiative. The completion of the reform and modernization of the United States export control system is imperative to ensuring that U.S. companies continue to be competitive in the current global economy.

As you know, the interagency task force has been reviewing the United States Munitions List (USML) and the Bureau of Industry and Security (BIS) Commerce Control List (CCL) so that the two lists may be rationalized and dual use items for the commercial market currently on the USML may be placed on the CCL, where they can be controlled by the appropriate entity, while keeping defense articles on the USML.

It is my understanding that the interagency review of the controls list and the stakeholder agreements have been complete for categories I-III for more than three years, but have yet to be published for public comment. I urge you to work in an expedited manner to complete the review of the remaining categories of the USML.

Thank you for your attention to this important matter. I look forward to your replies.

Sincere regards,



Roy Blunt
United States Senator



United States Department of State

Washington, D.C. 20520

The Honorable
Roy Blunt
United States Senate
Washington, DC 20510

FEB 05 2016

Dear Senator Blunt:

Thank you for your October 7, 2015 letter expressing support for the President's Export Control Reform (ECR) Initiative. The Initiative is vital to U.S. national security and foreign policy interests. As you note, much progress has been made in advancing ECR to date, with 15 of the 21 U.S. Munitions List Categories revised. We have also made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).

The Department is focused on continuing this effort successfully. We are working toward reviewing the remaining USML categories, while beginning to re-review those that were last revised over two years ago. Additionally, our efforts include further work to clarify and harmonize certain definitions in the ITAR and the EAR, which was the subject of a recent proposed rule.

At this time, the Department's primary focus, as well as that of our interagency partners, is to finalize the significant number of proposed rule-makings currently in process, which include revisions to USML Categories XII and XIV. Nonetheless, the Department is committed to finalizing an initial review of the entire USML in 2016.

We appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Julia Frisfield".

Julia Frisfield
Assistant Secretary
Legislative Affairs

No. 15-50759

**In the
United States Court of Appeals
for the Fifth Circuit**

DEFENSE DISTRIBUTED AND SECOND AMENDMENT FOUNDATION, INC.,

PLAINTIFFS – APPELLANTS,

v.

U.S. DEPARTMENT OF STATE; JOHN F. KERRY, IN HIS OFFICIAL CAPACITY AS SECRETARY OF STATE; DIRECTORATE OF DEFENSE TRADE CONTROLS, DEPARTMENT OF STATE BUREAU OF POLITICAL MILITARY AFFAIRS; KENNETH B. HANDELMAN, INDIVIDUALLY AND IN HIS OFFICIAL CAPACITY AS DEPUTY ASSISTANT SECRETARY, DEFENSE TRADE CONTROLS, BUREAU OF POLITICAL MILITARY AFFAIRS, DEPARTMENT OF STATE; C. EDWARD PEAR-TREE, INDIVIDUALLY AND IN HIS OFFICIAL CAPACITY AS DIRECTOR, OFFICE OF DEFENSE TRADE CONTROLS POLICY, BUREAU OF POLITICAL MILITARY AFFAIRS, DEPARTMENT OF STATE; SARAH J. HEIDEMA, INDIVIDUALLY AND IN HER OFFICIAL CAPACITY AS DIVISION CHIEF, REGULATORY AND MULTILATERAL AFFAIRS, OFFICE OF DEFENSE TRADE CONTROLS POLICY, BUREAU OF POLITICAL MILITARY AFFAIRS, DEPARTMENT OF STATE; AND GLENN SMITH, INDIVIDUALLY AND IN HIS OFFICIAL CAPACITY AS SENIOR ADVISOR, OFFICE OF DEFENSE TRADE CONTROLS, BUREAU OF POLITICAL MILITARY AFFAIRS, DEPARTMENT OF STATE,

DEFENDANTS – APPELLEES.

**On Appeal from the United States District Court
for the Western District of Texas**

**Brief of the Cato Institute
as *Amicus Curiae* in Support of Plaintiffs-Appellants**

Ilya Shapiro
Counsel of Record
Randal J. Meyer (admission pending)
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org
rmeyer@cato.org

Supplemental Certificate of Interested Persons

Case 15-50759, *Defense Distributed, et al., v. U.S. Dep't of State et al.*

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

<u>Person or Entity</u>	<u>Connection to Case</u>
Ilya Shapiro	Counsel to <i>amicus</i>
Randal J. Meyer	Counsel to <i>amicus</i>
Cato Institute	<i>Amicus curiae</i>

Amicus curiae Cato Institute is a Kansas nonprofit corporation. It has no parent companies, subsidiaries, or affiliates. It does not issue shares to the public.

/s/ Ilya Shapiro

Table of Contents

	Page
Supplemental Certificate of Interested Persons	1
Table of Contents	2
Table of Authorities.....	3
Interest and Independence of <i>Amicus Curiae</i>	7
Summary of Argument.....	8
Argument.....	9
I. Defense Distributed’s Speech Does Not Lose First Amendment Protection Simply Because It Could Be Used Unlawfully	9
A. Defense Distributed’s Files Constitute Protected Speech	9
B. Protected Speech Does Not Lose First Amendment Protec- tion Simply Because It Could Be Used to Unlawful Ends	12
II. The State Department’s Categorical Ban on Distributing the CAD Files Via the Internet Is an Unlawful Prior Restraint on the Mass Dissemination of Protected Speech.....	24
A. The Internet Is an Essential Method of Mass Dissemina- tion, So a Prior Restraint on Its Use Is Suspect.....	24
B. Prior Restraint of the Mass Dissemination of Protected Speech Cannot Even Pass Rational Basis Review	26
Conclusion	31
Certificate of Compliance	32
Certificate of Filing and Service	32

Table of Authorities

Cases

<i>Ashcroft v. Free Speech Coalition</i> , 535 U.S. 234 (2002).....	<i>passim</i>
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001).....	22, 23, 30
<i>Brandenburg v. Ohio</i> , 395 U.S. 444 (1969) (per curiam)	9, 15, 18, 19, 23
<i>Broadrick v. Oklahoma</i> , 413 U.S. 601 (1973).....	15, 26, 29
<i>Brown v. Entm’t Merchants Ass’n</i> , 131 S. Ct. 2729 (2011).....	10
<i>Butler v. Michigan</i> , 352 U.S. 380 (1957).....	<i>passim</i>
<i>Chaplinsky v. New Hampshire</i> , 315 U.S. 568 (1942).....	23
<i>Cohen v. California</i> , 403 U.S. 15 (1971).....	17
<i>Defense Distributed v. U.S. Dep’t of State</i> , No. 1:15-CV-372 RP, 2015 WL 4658921 (W.D. Tex. Aug. 4, 2015)	10, 26
<i>Hess v. Indiana</i> , 414 U.S. 105 (1973) (per curiam)	15
<i>Junger v. Daley</i> , 209 F.3d 481 (6th Cir. 2000).....	10, 12

<i>Kingsley Int’l Pictures Corp. v. Regents of Univ. of N.Y.</i> , 360 U.S. 684 (1959).....	30
<i>Miller v. California</i> , 413 U.S. 15 (1973).....	23
<i>NAACP v. Claiborne Hardware Co.</i> , 458 U.S. 886 (1982).....	20, 27
<i>New York Times Co. v. Unites States</i> , 376 U.S. 254 (1964).....	19
<i>New York Times Co. v. Unites States</i> , 403 U.S. 713 (1971) (per curiam)	18, 19, 27-28, 30
<i>People v. Winters</i> , 294 N.Y. 545 (1945)	17
<i>Sable Communications of California, Inc. v. FCC</i> , 492 U.S. 115 (1989).....	21, 22, 28
<i>Scales v. United States</i> , 367 U.S. 203 (1961).....	21
<i>Schneider v. State</i> , 308 U.S. 147 (1939).....	16, 25, 27, 30
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2d Cir. 2001)	10
<i>Winters v. New York</i> , 333 U.S. 507 (1948).....	17
Statutes	
18 U.S.C. § 2256(B), (D) (2000)	14-15

22 U.S.C. §§ 2771-82 (2015)	8
22 U.S.C. § 2778(a)-(e) (2014)	30
Michigan Penal Code § 343 (1955).....	18
N.Y Penal Law § 1141(2) (McKinney’s 1947)	17

Other Authorities

22 C.F.R. 120.1(a) (2015).....	8
49 Fed. Reg. 47,682, 47,683 (Dec. 6, 1984)	9
55 Cong. Rec. 2009 (1917) (remarks of Sen. Henry F. Ashurst)	20
Aaron Mamiit, <i>3.2 Billion: Number Of People Using The Internet Today</i> , Tech Times (May 28 2015), http://www.techtimes.com/articles/55773/20150528/3-2-billion-number-of-people-using-the-internet-today.htm	24
Andy Greenberg, <i>3D-Printed Guns As Art: London Design Museum Buys Two ‘Liberator’ Printed Pistols</i> , Forbes (Sept. 15, 2013), http://www.forbes.com/sites/andygreenberg/2013/09/15/3d-printed-guns-as-art-london-design-museum-buys-two-liberator-printed-pistols	12, 22
Defendant’s Opposition to Plaintiff’s Motion For a Preliminary Injunction, <i>Defense Distributed v. U.S. Dep’t of State</i> , No. 1:15-CV-372 RP, 2015 WL 4658921 (W.D. Tex. Aug. 4, 2015).....	13
D.J. Pangburn, <i>3D-Printed ‘Liberator’ Guns Become a Chandelier Sculpture</i> , The Creators Project (Aug. 6, 2015), http://thecreatorsproject.vice.com/blog/3d-printed-liberator-guns-become-a-chandelier-sculpture	11

Eugene Volokh, <i>Crime-Facilitating Speech</i> , 57 Stan. L. Rev. 1096 (2005)	13-14
<i>How Americans Get Their News</i> , American Press Inst., (Mar. 17, 2014), http://www.americanpressinstitute.org/publications/reports/ survey-research/how-americans-get-news	25
<i>Internet 2012 in Numbers</i> , Pingdom.com (January 16, 2013), http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers	24
<i>Internet Users</i> , Internet Live Statistics (last updated July 1, 2014), http://www.internetlivestats.com/internet-users	24
Natasha Lennard. <i>The Pirate Bay Steps in to Distribute 3-D Gun Designs</i> , Salon (May 10, 2013), http://www.salon.com/2013/05/10/ the_pirate_bay_steps_in_to_distribute_3d_gun_designs	31
Scott J. Grunewald, <i>American Gun Show Uses Art and 3D Printing to Start a Conversation about Guns</i> , 3D Print.com (Nov. 11, 2015), http://3dprint.com/104975/american-gun-show-art	11
St. George Tucker, 2 Blackstone’s Commentaries on the Laws of England with Notes of Reference, to the Constitution and Laws, of the Federal Government of the United States, and the Commonwealth of Virginia (1803)	28

Interest and Independence of *Amicus Curiae*

The Cato Institute is a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Center for Constitutional Studies was established in 1989 to help restore the principles of constitutional government that are the foundation of liberty. Toward those ends, Cato publishes books and studies, conducts conferences, and publishes the annual *Cato Supreme Court Review*.

This case concerns *amicus* because protecting the fundamental rights to freedom of expression and armed self-defense lies at the heart of Cato's mission. It is not for the State Department to abrogate lawful First Amendment speech as a vehicle for suppressing the disfavored exercise of Second Amendment rights.

No one other than the *amicus* and its counsel wrote this brief in whole or in part. The cost of its preparation was paid solely by *amicus*.

The parties have consented to the filing of this brief.

SUMMARY OF ARGUMENT

Defense Distributed, a nonprofit organization that promotes popular access to constitutionally protected firearms, generates and disseminates information over the Internet for a variety of scientific, artistic, and political reasons. The State Department has required Defense Distributed to submit to a regulatory prior restraint on Internet distribution of certain CAD (Computer-Aided Drafting) files—complex three-dimensional printing files with no intellectual-property protection—even domestically, under the Arms Export Control Act (AECA) and International Trafficking in Arms Regulations (ITAR). *See generally* 22 U.S.C. §§ 2771-82 (2015); 22 C.F.R. 120.1(a) (2015).

But Defense Distributed's protected speech cannot be suppressed merely because the lawful CAD files may potentially be used for unlawful purposes by foreign third parties. Such a prior restraint cannot even pass rational basis review. This court should reverse the district court and grant a preliminary injunction.

ARGUMENT

I. DEFENSE DISTRIBUTED’S SPEECH DOES NOT LOSE FIRST AMENDMENT PROTECTION SIMPLY BECAUSE IT COULD BE USED UNLAWFULLY

The government concedes that Defense Distributed’s files are protected speech under ITAR. *See* 49 *Fed. Reg.* 47,682, 47,683 (Dec. 6, 1984) (addressing congressional “[c]oncerns” over “[ITAR] licensing requirements as they relate[] to the First Amendment,” and noting that there is no “prepublication review requirement” under AECA or ITAR for technical information distributed domestically). Because foreign persons may *potentially* download the files and use them for *potentially* illegal ends, however, the State Department imposed a prior restraint against Defense Distributed’s sharing of certain files with Americans. But the Supreme Court has made clear that speech does not lose First Amendment protection merely because it might be used to further criminal ends. *See generally, e.g., Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002); *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

A. Defense Distributed’s Files Constitute Protected Speech

Defense Distributed is not in the business of distributing arms. What it distributes—as recognized by the court below—is computer code and other expressive files. Such code and files are speech for First

Amendment purposes. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 447 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000). The Supreme Court has also held that the First Amendment protects the expression rendered by videogame computer code. *See Brown v. Entm't Merchants Ass'n*, 131 S. Ct. 2729, 2733 (2011) (“Like the protected books, plays, and movies that preceded them, video game [code] communicate[s] ideas—and even social messages . . . through features distinctive to the medium That suffices to confer First Amendment protection.”). When information is distributed in an open-source format, as Defense Distributed’s is, it is a public work that users are encouraged to improve and modify. *Defense Distributed v. U.S. Dep’t of State*, No. 1:15-CV-372 RP, 2015 WL 4658921, at *6 (W.D. Tex. Aug. 4, 2015) (“[T]he files are intended to be used by others as a baseline to be built upon, altered and otherwise utilized.”).

Taken as a whole, the files distributed by Defense Distributed have lead to significant political, scientific, and artistic expression, including driving the novel field of 3D-printed art. Computer code, including in the form of CAD files, is simply a medium through which expres-

sion occurs—and open-source code provides an open canvas for artists and technicians to improve upon.

Artists have even exhibited 3D-printed modifications of Defense Distributed’s “Liberator” model, “attempting to start a conversation about the United States’ obsession with guns, not by focusing on one side of the issue, but by bringing artists from both sides together and exposing the entirety of the complexity of the issue.” Scott J. Grunewald, *American Gun Show Uses Art and 3D Printing to Start a Conversation about Guns*, 3D Print.com (Nov. 11, 2015), <http://3dprint.com/104975/american-gun-show-art>. At another show, one artist, Addie Wagenknecht, took 13 3D-printed Liberator models and “assemble[d] them into a striking sculpture [a chandelier] that is equal parts futuristic, menacing, and comically absurd.” D.J. Pangburn, *3D-Printed ‘Liberator’ Guns Become a Chandelier Sculpture*, The Creators Project (Aug. 6, 2015), <http://thecreatorsproject.vice.com/blog/3d-printed-liberator-guns-become-a-chandelier-sculpture>.¹

¹ In fact, Wagenknecht “didn’t have a 3D printer so I had a friend print them for me in Germany” from a “torrent” of the CAD file (a special “mirrored” type of file that contains metadata but not content). *Id.* If the State Department’s argument is correct, she thus unwittingly became an international arms trafficker.

Indeed, London's Victoria & Albert Museum of Art and Design purchased two Liberator pistols from Defense Distributed for a design festival. Andy Greenberg, *3D-Printed Guns As Art: London Design Museum Buys Two 'Liberator' Printed Pistols*, *Forbes* (Sept. 15, 2013), <http://www.forbes.com/sites/andygreenberg/2013/09/15/3d-printed-guns-as-art-london-design-museum-buys-two-liberator-printed-pistols>. Cody Wilson, Defense Distributed's founder, told a reporter "that he's happy to see his 3D-printed gun recognized by the museum as the incendiary political symbol he's always intended it to be." *Id.*

As courts have properly recognized, computer code "has both an expressive feature and a functional feature." *Junger*, 209 F.3d at 485. Open-source CAD files, like the Liberator's, are a unique medium of expression and are integral to the development of the burgeoning field of 3D-design art, as well as 3D technical design itself. Accordingly, the open-source CAD files are protected speech.

B. Protected Speech Does Not Lose First Amended Protection Simply Because It Could Be Used to Unlawful Ends

The government defends its prior restraint of domestic public speech on the Internet with the vague-at-best claim that Defense Distributed's files *could* produce weapons that *could* be used to commit

crimes *outside* the United States. Defendant’s Opposition to Plaintiff’s Motion for a Preliminary Injunction 10, *Defense Distributed*, 2015 WL 4658921 (“The unrestricted provision of such undetectable firearms by U.S. persons to individuals in other countries . . . presents a serious risk of acts of violence in those countries . . . [such as] an assassination, for the manufacture of spare parts by embargoed nations, terrorist groups, or guerilla groups, or to compromise aviation security . . .”). Just because lawful computer code can be used in a potentially unlawful manner by foreign persons does not constitutionally permit the executive to impose a prior restraint on Americans’ expression. *See, e.g., Free Speech Coalition*, 535 U.S. at 245 (“The prospect of crime, however, by itself does not justify laws suppressing protected speech.”); *see also* the slew of Supreme Court precedents discussed *infra* in this section.

“[R]estrictions on [lawful] . . . speech [that could potentially be used unlawfully] can’t be easily justified under existing First Amendment doctrine.” Eugene Volokh, *Crime-Facilitating Speech*, 57 Stan. L. Rev. 1096, 1105 (2005). Consider that “[a] textbook, magazine, Web site, or seminar describ[ing] how people can make bombs (conventional or nuclear), make guns, make drugs . . . painlessly and reliably commit su-

icide . . . pick locks . . . or more effectively resist arrest during civil disobedience” has academic and scientific speech value, but could potentially be used for unlawful conduct. *See id.* at 1097, 1111-14. Indeed,

Books about explosives can teach students principles of chemistry, and can help engineers use explosives for laudable purposes. Books that explain how to investigate arson, homicide, or poisoning can help detectives and would-be detectives, though they can also help criminals learn how to avoid detection.

Id. at 1112. And “[s]cientific research,” like the computer science and 3D engineering research developed in modifying and examining open source code for computer CAD files, “is generally thought to advance more quickly when scientists and engineers are free to broadly discuss their work.” *Id.* To enact a prior restraint on all of these because of potential and non-specific unlawful uses by foreign individuals is “[s]urely . . . to burn the house to roast a pig.” *Butler v. Michigan*, 352 U.S. 380, 383 (1957). Numerous Supreme Court cases have agreed, including several *per curiam* opinions.

In *Free Speech Coalition*, for example, the Court struck down a prior restraint on pornography that “appears to be” or “conveys the impression” that the actors in the work are minors, whether or not those actors were in fact consenting adults. 535 U.S. at 258; 18 U.S.C.

§ 2256(B), (D) (2000). The government justified its prior restraint on the “ground that it may encourage pedophiles to engage in illegal conduct.” *Free Speech Coalition*, 535 U.S. at 254. The Court struck down the ban in light of the fact that “[t]he harm does not necessarily follow from the speech, but depends on some unquantified potential for subsequent criminal acts,” and that “the government may not prohibit speech because it increases the chance an unlawful act will be committed ‘at some indefinite time in the future.’” *Id.* at 250, 253 (quoting *Hess v. Indiana*, 414 U.S. 105, 108 (1973) (per curiam) and citing *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam)).

As the *Free Speech Coalition* Court declared: “the mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it,” and that “[p]rotected speech does not become unprotected merely because it resembles the latter. The Constitution requires the reverse.” *Id.* at 253, 255 (quoting and citing *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973)). Similarly, Defense Distributed’s speech is significantly attenuated from the potential harm and, accordingly, the government may not prohibit it.

The principle employed in *Free Speech Coalition* comes from a long line of Supreme Court precedent, dating back to the 1930s. In 1939, the Court addressed the question of municipal prior restraints on the distribution of handbills in public areas. Four municipalities argued that handbills could thus be restrained because of their potential to contribute to littering. *Schneider v. State*, 308 U.S. 147, 162 (1939) (“The motive of the legislation under attack . . . is held by the courts below to be the prevention of littering of the streets and, although the alleged offenders were not charged with themselves scattering paper in the streets, their convictions were sustained upon the theory that distribution by them encouraged or resulted in such littering.”). The Court held that “the purpose to keep the streets clean and of good appearance is insufficient to justify an ordinance which prohibits a person rightfully on a public street from handing literature to one willing to receive it.” *Id.* at 163. In other words, the Court stopped on First Amendment grounds the restriction of an essential method of mass dissemination of speech whose sole justification had been to prevent unlawful behavior.

In 1948, the Court faced an overbreadth challenge to New York’s anti-crime literature law, a prior restraint that made it a misdemeanor

to publish media “principally made up of criminal news, police reports, or accounts of criminal deeds, or pictures, or stories of deeds of bloodshed, lust or crime.” *Winters v. New York*, 333 U.S. 507, 508 (1948) (quoting N.Y. Penal Law § 1141(2) (McKinney’s 1947)). New York argued that crime literature could become “vehicles for inciting violent and depraved crime” at some future time among some indefinite individuals. *Id.* at 513 (quoting *People v. Winters*, 294 N.Y. 545, 550 (1945)).

The Court made short work of New York’s argument, noting that “[w]hat is one man’s amusement, teaches another doctrine . . . [the works at issue] are as much entitled to the protection of free speech as the best of literature.” *Id.* at 510; *see also Cohen v. California*, 403 U.S. 15, 25 (1971) (“[I]t is nevertheless often true that one man’s vulgarity is another’s lyric.”). The Court continued: “On its face, the subsection here involved violates the rule . . . that statutes which include prohibitions of acts fairly within the protection of a free press are void. It covers detective stories, treatises on crime, reports of battle carnage, et cetera.” *Id.* at 512. Even an authoritative limiting construction by the New York Court of Appeals was not sufficient to save the statute from the overbreadth challenge. *Id.* at 514-516, 518-20.

In 1957, Justice Frankfurter wrote for the Court to strike down a Michigan ban on disseminating literature that could have a “potentially deleterious influence upon youth,” such as “tending to incite minors to violent or depraved or immoral acts.” *Butler*, 352 U.S. at 381, 383 (quoting Michigan Penal Code § 343 (1955)). The legislation in that case was “not reasonably restricted to the evil with which it is said to deal.” *Id.* at 383. It “arbitrarily curtails” the freedom of speech, something that “history has attested as the indispensable condition for the maintenance and progress of a free society.” *Id.* at 384. Again the Court made clear that the mere potential for lawful speech to facilitate unlawful acts was an insufficient justification by itself for a prior restraint.

Two of the most important precedents in this line of cases followed: *Brandenburg v. Ohio*, 395 U.S. 444 (1969) (per curiam), and *New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam). *Brandenburg* provides a baseline for judging statutes that prohibit protected speech because of the chance it could encourage crime. In that case, a Klansman was charged with violating Ohio’s Criminal Syndicalism Statute for a political speech encouraging an armed march on Congress. *Brandenburg*, 395 U.S. at 444-47. The Court held that, unless

such encouragement is “inciting or producing imminent lawless action and is likely to incite or produce such action,” it is protected by the First Amendment. *Id.* at 447.

In *New York Times*, the Court held that a prior restraint injunction was not justified on the printing of the then-classified Pentagon Papers by the *Times* and the *Washington Post*. *New York Times*, 403 U.S. at 714. Individual justices had much more to say about suppressing lawful speech to stop potential and non-specific unlawful uses. Justice Black, joined by Justice Douglas, wrote a concurrence to note that public discourse should be “uninhibited, robust, and wide-open.” *Id.* at 724 (Black, J., concurring) (quoting *New York Times Co. v. Sullivan*, 376 U.S. 254, 269-70 (1964)). Moreover, “[t]he word ‘security’ is a broad, vague generality” that cannot simply be used as a talismanic incantation to permit a prior restraint on speech. *Id.* at 719.

Justice Brennan noted that the “First Amendment tolerates absolutely no prior judicial restraints . . . predicated upon surmise or conjecture that untoward consequences may result.” *Id.* at 725-26 (Brennan, J., concurring). Justice Stewart, joined by Justice White, evoked the *Brandenburg* majority when he noted that because he “cannot say that

disclosure of any of them will surely result in direct, immediate, and irreparable damage,” the First Amendment protects the distribution of the then-classified information. *Id.* at 730 (Stewart, J., concurring). Justice White, joined in turn by Justice Stewart, contrasted the blanket prior restraint in the case with the criminal sanctions imposed by statutes that relate to imminently harmful information like “movements of the fleet, the troops, the aircraft, the location of powder factories, the location of defense works, and all that sort of thing.” *Id.* at 734-35 (White, J., concurring) (quoting 55 Cong. Rec. 2009 (1917) (remarks of Sen. Henry F. Ashurst)). Accordingly, Justice White found that the prior restraint in that case could not pass constitutional muster because it was not sufficiently narrow to touch on those circumstances of actual imminent harm and there were sufficient criminal statutes to deter bad conduct. *See id.* at 735-40.

A decade later, the Court held that, despite the fact there were individual acts of violence involved in the political speech of the seven-year boycott of white-owned businesses in Claiborne County, Mississippi, the boycott’s overall speech was protected by the First Amendment. *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 915 (1982). While the

lawful speech tangentially encouraged unlawful acts by virtue of the tension created by the boycott itself, the speech was nevertheless protected. *Id.* at 933 (“The use of speeches, marches, and threats of social ostracism cannot provide the basis for a damages award. But violent conduct is beyond the pale of constitutional protection.”) The Court took into account that “‘blanket prohibition of association with a group having both legal and illegal aims’ would present ‘a real danger that legitimate political expression or association would be impaired.’” *Id.* at 919 (quoting *Scales v. United States*, 367 U.S. 203, 229 (1961)).

In 1989, the Court again protected lawful speech from indefinite and vague claims that it could be used for unlawful purposes. *Sable Communications of Calif., Inc. v. FCC*, 492 U.S. 115 (1989). In *Sable Communications*, a federal ban on obscene telephone communications via interstate commerce criminalized all commercial phone-sex lines. *Id.* at 123 (quoting 47 U.S.C § 223(b) (1988)). The reason for the blanket prior restraint was to “restrict access to minors” to phone-sex services. *Id.* at 122-23. In striking down the ban, the Court expressly relied on *Butler*. See, e.g., *id.* at 131 (quoting *Butler*, 352 U.S. at 383).

Similar to the restraint struck down in *Claiborne Hardware*, the Liberator files should not be subject to blanket prohibition of Internet dissemination, lest legitimate expression be chilled. *See* Greenberg, *3-D Printed Guns as Art*; *supra* Part I.A (noting artistic, scientific, and political uses of the computer-code speech). And similar to the restrictions in *Butler* and *Sable Communications*, the prior restraint on Americans' viewing Defense Distributed's files online impermissibly limits U.S. audiences to speech suitable for foreign audiences. *Cf. Sable*, 492 U.S. at 127 ("The Court found the law to be insufficiently tailored since it denied adults their free speech rights by allowing them to read only what was acceptable for children.") (quoting *Butler*, 352 U.S. at 380)); *Butler*, 352 U.S. at 383-84 ("The incidence of this enactment is to reduce the adult population of Michigan to reading only what is fit for children. It thereby arbitrarily curtails one of those liberties of the individual . . .").

The Court has even more recently reaffirmed the basic principle that lawful speech cannot be suppressed in order to prevent potential unlawful uses. In *Bartnicki v. Vopper*, the Court was "firmly convinced" that "a stranger's illegal conduct does not suffice to remove the First Amendment protection shield from speech." 532 U.S. 514, 518, 535

(2001); *see also id.* at 529-30 (“[I]t would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party.”). *Bartnicki* asked whether the First Amendment protected a radio station from suit when it broadcasted the results of illegally intercepted communications. *Id.* at 519-20. The government’s interest in allowing the private action against the publisher rested in discouraging illegal conduct such as eavesdropping. *See id.* at 521-24. Yet again, the interest in discouraging potential illegal conduct was not sufficient to warrant restricting protected First Amendment expression. Such an interest is likewise insufficient to restrain the distribution of open-source files.

In sum, while the government certainly has the power to constraint certain categories of speech, like obscenity and the urging of imminent violence, those categories are specific and narrowly drawn. *See generally Miller v. California*, 413 U.S. 15 (1973) (obscenity); *Brandenburg*, 395 U.S. at 444 (instigating violence); *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942) (fighting words). Here the government has presented no evidence to demonstrate the instigation of imminent violence or invoke any other categorical prohibition.

II. THE STATE DEPARTMENT'S CATEGORICAL BAN ON DISTRIBUTING THE CAD FILES VIA THE INTERNET IS AN UNLAWFUL PRIOR RESTRAINT ON THE MASS DISSEMINATION OF PROTECTED SPEECH

The Internet is an essential method of mass dissemination beyond the scale of newspapers and television. A prior restraint on lawful speech uploaded online cannot even pass rational basis review when the harm of potential unlawful action is attenuated and non-specific.

A. The Internet Is an Essential Method of Mass Speech Dissemination, So a Prior Restraint on Its Use Is Suspect

It has quickly become axiomatic that a prior restraint on Internet communications cuts off an incomparably important avenue for American expression. Consider the following data points, all of which have become quickly dated:

- The total number of Internet users worldwide has reached over 3.2 billion. Aaron Mamiit, *3.2 Billion: Number of People Using the Internet Today*, Tech Times (May 28, 2015), <http://www.techtimes.com/articles/55773/20150528/3-2-billion-number-of-people-using-the-internet-today.htm>.
- Of the total American population, 86.75 percent have Internet access, about 280 million users. *Internet Users*, Internet Live Statistics (last updated July 1, 2014), <http://www.internetlivestats.com/internet-users>.
- In 2012, there were 634 million websites, with 50 million new sites added per month. *Internet 2012 in Numbers*, Pingdom.com (January 16, 2013), <http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers>.

- The U.S. hosted 43 percent of the top million websites that year. *Id.*
- Sixty-nine percent of Americans get news from the Internet. *How Americans Get Their News*, American Press Inst. (Mar. 17, 2014), www.americanpressinstitute.org/publications/reports/survey-research/how-americans-get-news.

Suffice it to say, the Internet is a revolutionary means of mass communications, so speech restrictions must be drawn with surgical precision.

In striking down municipal ordinances prohibiting the distribution of handbills in *Schneider*, for example, the Supreme Court was not persuaded that laws should be upheld “because their operation is limited to streets and alleys and leaves persons free to distribute printed matter in other public places.” *Schneider*, 308 U.S. at 163. “[T]he streets,” wrote the Court, “are natural and proper places for the dissemination of information and opinion; and one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place.” *Id.* Meanwhile, pamphlets deserve special solicitude because they are “effective instruments in the dissemination of opinion.” *Id.* at 164.

In the rare cases where the Court has upheld prior restraints, these restrictions were narrowly tailored rather than applied to broad

channels of speech dissemination. In *Broadrick v. Oklahoma*, for example, the Court sustained an Oklahoma law that “restricts the political activities of the State’s classified civil servants in much the same manner that the Hatch Act proscribes partisan political activities of federal employees.” 413 U.S. 601, 602 (1973). The statute focused on electioneering activities and not the “right as a citizen privately to express his opinion and to cast his vote,” so the Court upheld the restriction because it “seeks to regulate political activity in an even-handed and neutral manner.” *Id.* at 606, 616.

In other words, a blanket prior restraint on an important channel of mass dissemination like the Internet is highly suspect.

B. Prior Restraint of the Mass Dissemination of Protected Speech Cannot Even Pass Rational Basis Review

Applying intermediate scrutiny, the court below found that Defense Distributed has “not shown a substantial likelihood of success on the merits of their claim under the First Amendment.” *Defense Distributed*, 2015 WL 4658921, at *10. Even though “the AECA and ITAR do not prohibit domestic communications,” under the ITAR, the dissemination of the open source CAD files is an “export” of technical arms information according to the government, and thus subject to prepublication

commodity jurisdiction review and prior restraint without agency approval. *See id.* Even if the government were correct in its view on what constitutes an “export,” however, such a prior restraint on protected speech cannot even pass rational basis review.

As discussed more fully *supra* at I.B, the Supreme Court has overturned prior restraints similar to the one in this case. In *Schneider*, the Supreme Court disagreed with the court below that a prohibition on distributing handbills in public fora “does not transgress the bounds of reasonableness.” 308 U.S. at 155. In *Butler*, the Court found that a prior restraint on adult-appropriate obscene literature in order to avoid potential unlawful use by minors was “[s]urely . . . to burn the house to roast the pig.” 352 U.S. at 381-83.

A blanket prior restraint that sweeps in the online dissemination of protected public domestic speech lacks the “precision of regulation” sufficient to pass even rational basis review. *See Claiborne Hardware*, 458 U.S. at 916 (quoting *NAACP v. Button*, 371 U.S. 415, 438 (1963)); *Butler*, 352 U.S. at 381-83; *Schneider*, 308 U.S. at 155; *see also Free Speech Coalition*, 535 U.S. at 252 (affirming the same under heightened scrutiny). *New York Times* subsequently upheld the “heavy presump-

tion” against prior restraints on lawful speech has the potential for unlawful uses. *See New York Times Co.*, 403 U.S. at 731, 733 (White, J., concurring).² In several subsequent cases the Court made specific note of its strong distaste for prior restraints. In *Sable Communications*, the Court took its conclusion directly from *Butler* in striking down the federal phone-sex ban, referencing the rational basis standard: “As Justice Frankfurter said in that case, ‘[s]urely, this is to burn the house to roast the pig.’ In our judgment, this case, like *Butler*, presents us with ‘legislation not reasonably restricted to the evil with which it is said to deal.’” 492 U.S. at 127 (quoting and citing *Butler*, 352 U.S. at 383). In *Free Speech Coalition*, the Court again clarified that “[t]he evil in question

² A “heavy presumption” against prior restraints is as old as the nation itself:

That where absolute freedom of discussion is prohibited, or restrained, responsibility vanishes. That any attempt to prohibit, or restrain that freedom, may well be construed to proceed from conscious guilt. That the people of America have always manifested a most jealous sensibility, on the subject of this inestimable right, and have ever regarded it as a fundamental principle in their government, and carefully engrafted in the constitution.

St. George Tucker, 2 Blackstone’s Commentaries on the Laws of England with Notes of Reference, to the Constitution and Laws, of the Federal Government of the United States, and the Commonwealth of Virginia App. at Note G, 16-17. (1803); *see also id.* at 17 (noting that even for proponents of the Alien and Sedition Acts of 1798, “[T]he liberty of the press consists not in a license for every man to publish what he pleases . . . but in a permission to publish without previous restraint.”).

depends upon the actor's unlawful conduct, conduct defined as criminal quite apart from any link to the speech in question. This established that the speech ban is not narrowly drawn." 535 U.S. at 252.

Even in cases approving of prior restraints, the Court is very careful to note the *extremely* narrow nature and impact of the holding. For example, in *Broadrick*, the Court upheld a prior restraint on election activities by civil servants. 413 U.S. 601. The Court there specifically noted that petitioner's activities (fundraising for their own superior at work) fell "squarely within the 'hard core' of the statute," and that the state regulator and attorney general had "construed 818's explicit approval of private political expression to include virtually any expression not within the context of active partisan political campaigning." *Id.* at 608, 617. Indeed, the Court pointed out that the prior restraint was not so broad as to cover "the wearing of political buttons or the use of bumper stickers"—thus substantially keeping open the marketplace of ideas. *See id.* at 618.

Moreover, blanket prior restraints like this one are typically appropriate only in the absence of a criminal statute. *See, e.g., Free Speech Coalition*, 535 U.S. at 245 ("Among free men, the deterrents ordinarily

to be applied to prevent crime are education and punishment for violations of the law, not abridgement of the rights of free speech.”) (quoting *Kingsley Int’l Pictures Corp. v. Regents of Univ. of N.Y.*, 360 U.S. 684, 689 (1959)); *Bartnicki*, 532 U.S. at 529 (“the normal method of deterring unlawful conduct is to impose an appropriate sanction on the person who engages in it. If the sanctions that presently attach to a violation . . . do not provide sufficient deterrence, perhaps those sanctions should be made more severe.”); *Schneider*, 308 U.S. at 162 (“There are obvious methods of preventing littering. Amongst these is punishment of those who actually throw paper on the streets.”); *New York Times Co.*, 403 U.S. at 734-40 (White, J., concurring). To justify a prior restraint, those criminal statutes must be shown to be incapable of preventing the evil at which it is aimed.

Here, all of the potential harms that concern the government are already criminalized. There is an applicable criminal law that targets the foreign export of arms-constructing information, with penalties of up to 20 years’ imprisonment and a million dollar fine. 22 U.S.C. § 2778(a)-(e) (2014). To justify its prior restraint, the government must show that it would be the only effective method to prevent such ex-

ports—as compared to the criminal statute and any narrower regulations. The government has not met and cannot meet that burden.³

CONCLUSION

For the foregoing reasons, *amicus* urges the court to reverse the district court and grant the motion for a preliminary injunction.

Respectfully submitted,

/s/ Ilya Shapiro

Ilya Shapiro

Counsel of Record

Randal J. Meyer (admission pending)

CATO INSTITUTE

1000 Mass. Ave., N.W.

Washington, D.C. 20001

(202) 842-0200

ishapiro@cato.org

rmeyer@cato.org

³ The government especially cannot meet this burden when an artist—decidedly not a sophisticated arms dealer—can evade the prior restraint by otherwise acquiring the file that is purportedly made unavailable and sending it to a foreign friend to 3D-print. *See supra* note 1 and accompanying text. The CAD files that Defense Distributed is restrained from distributing online are now widely available as downloadable torrent files. Natasha Lennard, *The Pirate Bay Steps in to Distribute 3-D Gun Designs*, Salon (May 10, 2013), http://www.salon.com/2013/05/10/the_pirate_bay_steps_in_to_distribute_3d_gun_designs.

Certificate of Compliance

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 4,975 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it was prepared using Word 2010 and uses a proportionally spaced typeface, Century Schoolbook, in 14-point type for body text and 12-point type for footnotes.

/s/ Ilya Shapiro

Certificate of Filing and Service

On December 17, 2015, I filed this *Brief of the Cato Institute as Amicus Curiae* using the CM/ECF System, which will send a Notice of Filing to all counsel of record.

/s/ Ilya Shapiro

Case No. 15-50759

**UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT**

DEFENSE DISTRIBUTED; SECOND AMENDMENT FOUNDATION,
INCORPORATED,

Plaintiffs-Appellants,

v.

UNITED STATES DEPARTMENT OF STATE; JOHN F. KERRY, In His Official Capacity as the Secretary of the Department of State; DIRECTORATE OF DEFENSE TRADE CONTROLS, Department of State Bureau of Political Military Affairs; KENNETH B. HANDELMAN, Individually and in His Official Capacity as the Deputy Assistant Secretary of State for Defense Trade Controls in the Bureau of Political-Military Affairs; C. EDWARD PEARTREE, Individually and in His Official Capacity as the Director of the Office of Defense Trade Controls Policy Division; SARAH J. HEIDEMA, Individually and in Her Official Capacity as the Division Chief, Regulatory and Multilateral Affairs, Office of Defense Trade Controls Policy; GLENN SMITH, Individually and in His Official Capacity as the Senior Advisor, Office of Defense Trade Controls,

Defendants-Appellees.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS, AUSTIN DIVISION
IN CASE NO. 15-CV-00372, THE HONORABLE ROBERT PITMAN

**BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF PLAINTIFFS-APPELLANTS**

Kit Walsh (CA SBN 303598)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
kit@eff.org

December 17, 2015

Counsel for Amicus Curiae

SUPPLEMENTAL STATEMENT OF INTERESTED PARTIES

Pursuant to this Court's Rule 29.2, the undersigned counsel of record for *amicus curiae* certifies that the following additional persons and entities have an interest in the outcome of this case.

1. Electronic Frontier Foundation, *amicus curiae*. Electronic Frontier Foundation is a nonprofit organization recognized as tax exempt under Internal Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.
2. Kit Walsh, attorney for *amicus curiae*.
3. Adam Schwartz, attorney for *amicus curiae*.

Dated: December 17, 2015

/s/ Kit Walsh

Kit Walsh

TABLE OF CONTENTS

SUPPLEMENTAL STATEMENT OF INTERESTED PARTIES	i
INTEREST OF <i>AMICUS CURIAE</i>	1
INTRODUCTION AND SUMMARY OF ARGUMENT	2
ARGUMENT.....	3
I. The Government Has Imposed a Prepublication Review Regime for Technical Information with Military Applications.	3
II. ITAR Restricts Protected Speech, Including the Defense Distributed Files.	6
A. Publishing Technical Information is Protected Speech.	6
B. Computer-Readable Documentation and Designs, Like Those of Defense Distributed, Are Protected Speech.	9
C. First Amendment Protection is Not Diminished For Speech That is Accessible to Foreigners.....	12
III. ITAR’s Prepublication Review of Technical Data Is an Unlawful Prior Restraint on Speech.....	13
A. Speech-Licensing Regimes that Lack Procedural Safeguards are Invalid.....	13
B. ITAR’s Prepublication Review Scheme Lacks the Required Safeguards.	16
C. The Government Incorrectly Argues that ITAR Prepublication Review is Not a Prior Restraint.	17
IV. The Government Cannot Show that the Speech Burdened by Prepublication Review Would Cause Direct, Immediate, and Irreparable Harm to National Security.....	19
V. ITAR’S Ban on Publications IS a Content-Based Regulation that Fails Strict Scrutiny.....	21

A. ITAR Is a Content-Based Regulation of Speech.	21
B. ITAR Does Not Satisfy Strict Scrutiny.....	24
1. Less-Restrictive Means Are Available to Address ITAR’s Goals.....	25
2. Most Speech Burdened by ITAR Does Not Threaten Any Concrete Government Interest.....	28
3. Alternative Channels for Speech Do Not Justify the Restraint.....	29
VI. The Prepublication Review Scheme Is Invalid Even Under the Reduced Scrutiny the Government Advocates.	30
CONCLUSION.....	31
CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION.....	33
CERTIFICATE OF SERVICE.....	34

TABLE OF AUTHORITIES

Cases

<i>Am. Booksellers Ass'n. v. Hudnut</i> , 771 F.2d 323 (7th Cir. 1985).....	8
<i>Ashcroft v. Free Speech Coal.</i> , 535 U.S. 234 (2002)	8
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001)	7, 8
<i>Bd. of Trs. of Leland Stanford Jr. Univ. v. Sullivan</i> , 773 F. Supp. 472 (D.D.C. 1991)	7
<i>Bernstein v. U.S. Dep't of State</i> , 922 F. Supp. 1426 (N.D. Cal. 1996)	11, 16
<i>Bernstein v. U.S. Dep't of State</i> , 974 F. Supp. 1288 (N.D. Cal. 1997)	14
<i>Boehner v. McDermott</i> , 484 F.3d 573 (D.C. Cir. 2007)	27
<i>Buckley v. Valeo</i> , 424 U.S. 1 (1976)	24
<i>Bullfrog Films, Inc. v. Wick</i> , 646 F. Supp. 492 (C.D. Cal. 1986).....	12
<i>Bullfrog Films, Inc., v. Wick</i> , 847 F.2d 502 (9th Cir. 1988).....	12
<i>Burson v. Freeman</i> , 504 U.S. 191 (1992)	22
<i>Cantwell v. Connecticut</i> , 310 U.S. 296 (1940)	22, 23
<i>CBS Inc. v. Davis</i> , 510 U.S. 1315 (1994)	19

<i>Consolidated Edison Co. of N.Y. v. Public Service Comm’n of N.Y.</i> , 447 U.S. 530 (1980)	22
<i>Dambrot v. Cent. Mich. Univ.</i> , 55 F.3d 1177 (6th Cir. 1995)	7
<i>Eu v. San Francisco County Democratic Cent. Committee</i> , 489 U.S. 214 (1989)	24
<i>FEC v. Mass. Citizens for Life, Inc.</i> , 479 U.S. 238 (1986)	24
<i>FEC v. Nat’l Conservative Political Action Comm.</i> , 470 U.S. 480 (1985)	24
<i>Fernandes v. Limmer</i> , 663 F.2d 619 (5th Cir. 1981)	16, 20
<i>First Nat’l Bank v. Bellotti</i> , 435 U.S. 765 (1978)	24
<i>Florida Star v. B.J.F.</i> , 491 U.S. 524 (1989)	24, 28
<i>Forsyth County v. Nationalist Movement</i> , 505 U.S. 123 (1992)	22, 23
<i>Freedman v. Maryland</i> , 380 U.S. 51 (1965)	<i>passim</i>
<i>FW/PBS, Inc. v. City of Dallas</i> , 493 U.S. 215 (1990)	13, 15
<i>Globe Newspaper Co. v. Superior Court for Norfolk</i> , 457 U.S. 596 (1982)	24
<i>Herceg v. Hustler Magazine, Inc.</i> , 814 F.2d 1017 (5th Cir. 1987)	8
<i>Jean v. Mass. State Police</i> , 492 F.3d 24 (1st Cir. 2007)	27

<i>Junger v. Daley</i> , 209 F.3d 481 (6th Cir. 2000).....	7, 11
<i>Kaplan v. California</i> , 413 U.S. 115 (1973)	9
<i>Lakewood v. Plain Dealer Pub. Co.</i> , 486 U.S. 750 (1988)	<i>passim</i>
<i>Marks v. United States</i> , 430 U.S. 188 (1977)	20
<i>McCullen v. Coakley</i> , 134 S. Ct. 2518 (2014)	31
<i>Meyer v. Grant</i> , 486 U.S. 414 (1988)	24
<i>Minneapolis Star & Tribune Co. v. Minnesota Comm’r of Revenue</i> , 460 U.S. 575 (1983)	23
<i>N.Y. Times Co. v. United States</i> , 403 U.S. 713 (1971)	19, 20
<i>Nat. Socialist Party of Am. v. Skokie</i> , 432 U.S. 43 (1977)	15
<i>Nebraska Press Ass’n v. Stuart</i> , 427 U.S. 539 (1975)	19, 20, 21
<i>R. A. V. v. City of St. Paul</i> , 505 U.S. 377 (1992)	24
<i>Reed v. Town of Gilbert</i> , 135 S. Ct. 2218 (2015)	22, 23
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997)	24, 29, 30
<i>Riley v. Nat’l Fed’n of Blind of N.C., Inc.</i> , 487 U.S. 781 (1988)	17

<i>Se. Promotions, Ltd. v. Conrad</i> , 420 U.S. 546, 553 (1975)	13
<i>Shuttlesworth v. City of Birmingham, Ala.</i> , 394 U.S. 147 (1969)	14
<i>Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.</i> , 502 U.S. 105 (1991)	22, 24
<i>Sorrell v. IMS Health Inc.</i> , 131 S. Ct. 2653 (2011)	6, 7, 21
<i>Turner Broad. Sys., Inc. v. F.C.C.</i> , 512 U.S. 622	31
<i>U.S. v. Playboy Entm't Grp., Inc.</i> , 529 U.S. 803 (2000)	24
<i>United States v. Chi Mak</i> , 683 F.3d 1126 (9th Cir. 2012)	18
<i>United States v. Edler Indus., Inc.</i> , 579 F.2d 516 (9th Cir. 1978)	18
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2d Cir. 2001)	11
<i>Winter v. G.P. Putnam's Sons</i> , 938 F.2d 1033	8

Federal Regulations

22 C.F.R. § 120.10	4, 6, 9
22 C.F.R. § 120.11	18, 25, 26
22 C.F.R. § 120.17	3, 6, 12, 30
22 C.F.R. § 120.4	5
22 C.F.R. § 121.1	4
22 C.F.R. § 123.1	5

22 C.F.R. § 126.7	5, 16, 17, 23
22 C.F.R. § 127.1	3
22 C.F.R. § 128.1	5, 17, 18
22 U.S.C. § 2778.....	3, 5, 18

Legislative Materials

Undetectable Firearms Modernization Act, H.R. 3643, 113th Cong. (2013).....	27
Undetectable Firearms Reauthorization Act, S.1774, 113th Cong (2013).	27

Other Authorities

<i>Commodity Jurisdiction Final Determinations</i> , U.S. Dep’t of State, Dir. of Def. Trade Controls.....	4
<i>DOJ Memos on ITAR Prior Restraint</i> , Defense Trade Law Blog, July 9, 2015	25
Elise Dalley, <i>Bypassing Geo-blocked Sites</i> , Choice, Aug. 13, 2014	30
hroncok, <i>Statue of Liberty with Base Building</i> , Thingiverse (Mar. 25, 2013).....	10
Information Policy & Access Center, 2014 Digital Inclusion Survey (2015)	26
Kasie Hunt & Carrie Dann, <i>Senate Extends Ban on Undetectable Guns But Nixes Tighter Restrictions</i> , NBC News, Dec. 9, 2013	27
Kathryn Zickuhr, et al., <i>Library Services in the Digital Age</i> , Pew Internet, Jan. 22, 2013	26
Policy on Review Time for License Applications, 74 Fed. Reg. 63,497 (Dec. 3, 2009).....	5, 17
Slic3r Home Page	10
Solid Cube, http://cpansearch.perl.org/src/EWILHELM/CAD-Format-STL- v0.2.1/files/cube.stl	10
U.S. Dep’t of State, <i>Munitions Control Newsletter</i>	25
Wai Hon Wah, <i>Introduction to STL format</i> , (June 1999)	10

INTEREST OF *AMICUS CURIAE*¹

Amicus Curiae is non-profit public interest organizations seeking to protect speech and innovation on the Internet.

The Electronic Frontier Foundation (“EFF”) is a non-profit, member-supported civil liberties organization that works to protect free speech, innovation, and privacy in the online world. With more than 22,000 dues-paying members, EFF represents the interests of technology users in both court cases and broader policy debates regarding the application of law in the digital age. EFF actively encourages and challenges industry and government to support free expression, innovation, privacy, and openness in the information society. EFF frequently participates, either as counsel of record or amicus, in cases involving the First Amendment and new technologies.

¹ Pursuant to Federal Rule of Appellate Procedure Rule 29(c), EFF certifies that no person or entity, other than amicus, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. Both Plaintiffs-Appellants and Defendants-Appellees consent to the filing of this brief. In the interest of full disclosure: EFF previously counseled Defense Distributed in regard to its first set of commodity jurisdiction requests, relating to certain files at issue in this case identified in Appellants’ brief as the “Published Files,” but EFF has not represented any party in connection with this litigation.

INTRODUCTION AND SUMMARY OF ARGUMENT

The First Amendment does not permit the government to presumptively criminalize online speech on a certain topic, and then decide on a case-by-case basis which speech to license, without any binding standards, fixed deadlines, or judicial review. Yet that is the regime advanced by the government in this case, criminalizing Americans who use the Internet to publish lawfully-obtained, nonclassified technical information relating to firearms and other technologies with military applications.

The licensing regime at issue in this case is a prior restraint that lacks the procedural safeguards required by the First Amendment to prevent discriminatory censorship decisions. It flies in the face of Supreme Court decisions that dictate how free speech interests are balanced with national security, such that speech is restrained only where absolutely necessary to prevent proven, immediate threats to concrete national security interests.

Beyond its flaws as a prior restraint, ITAR is a content-based regulation of speech that cannot survive strict scrutiny (or even the lesser scrutiny urged by the government) because it unnecessarily criminalizes a vast amount of protected speech that poses no risk to the putative goals of the regulatory regime. The regulation impermissibly sacrifices speech for the convenience of the government,

broadly criminalizing speech and putting the onus on speakers to seek leave to publish.

The Department of Justice warned the administrators of ITAR over thirty years ago that the First Amendment would not allow such a prepublication review regime. Yet, rather than developing appropriately-tailored regulations, the government has revived the overbroad scheme of prior restraint it once disavowed. The government will be unable to establish that this scheme is consistent with the First Amendment.

ARGUMENT

I. The Government Has Imposed a Prepublication Review Regime for Technical Information with Military Applications.

The International Traffic in Arms Regulations (ITAR) criminalize “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad” without a license. 22 C.F.R. §§ 120.17(a)(4), 127.1; 22 U.S.C. § 2778(c). Violations carry massive penalties: up to 20 years imprisonment and a \$1,000,000 fine. 22 U.S.C. § 2778(c).

Because the government considers electronic publication to be an “export,” it requires that Internet users submit publications for review by agency officials before they may electronically publish information that is considered “technical data.” 22 C.F.R. § 127.1. Technical data includes “[i]nformation . . . which is required for the design, development, production, manufacture, assembly,

operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.” 22 C.F.R. § 120.10(a)(1). Technical data also includes software. § 120.10 (a)(4). “Defense articles” refers to a list of technologies designated at the discretion of the Department of State in consultation with the Department of Defense, listed at 22 C.F.R. § 121.1 (the “United States Munitions List” or USML). In addition to firearms, the USML includes a range of medical, chemical, electronic, and mechanical engineering categories, and the open-ended provision that “[a]ny article not enumerated on the U.S. Munitions List may be included in this category” by the Director of the Office of Defense Trade Controls Policy. Category XXI(a).

Those who desire to publish information relating to controlled technologies must determine whether a license is needed for their disclosure. The scope of the regulation is sufficiently ambiguous that nearly four thousand “commodity jurisdiction” requests have been made since 2010 to clarify whether a particular technology would require a license.² These determinations are made “on a case-by-case basis, taking into account” nonbinding considerations such as “the nature, function and capability” of the civil and military applications of items described in

² *Commodity Jurisdiction Final Determinations*, U.S. Dep’t of State, Dir. of Def. Trade Controls, https://www.pmddtc.state.gov/commodity_jurisdiction/determinations.html

the technical data. 22 C.F.R. § 120.4(d). There are no firm deadlines for a final determination or resolution of an administrative appeal. 22 C.F.R. §§ 120.4 (e), (g). The decision “shall not be subject to judicial review.” 22 U.S.C. § 2778(h).

If the government decides that information is subject to ITAR, then the speaker must apply for a license to publish online. 22 C.F.R. § 123.1(a). No firm standards govern this process: “Any application for an export license or other approval under this subchapter may be disapproved . . . whenever: (1) The Department of State deems such action to be in furtherance of *world peace, the national security or the foreign policy* of the United States, *or is otherwise advisable.*” 22 C.F.R. § 126.7(a) (emphasis added). While the President has imposed a 60-day deadline to adjudicate applications, broad and open-ended exceptions swallow the rule. Policy on Review Time for License Applications, 74 Fed. Reg. 63,497 (Dec. 3, 2009). Adjudication may be indefinitely delayed whenever “[t]he Department of Defense has not yet completed its review” or “a related export policy is under active review and pending final determination by the Department of State.” *Id.* If a license is denied, an applicant may request reconsideration, but there is *no firm deadline* for action. *See* 22 C.F.R. § 126.7(c). There is also no opportunity for judicial review. 22 C.F.R. § 128.1.

II. ITAR Restricts Protected Speech, Including the Defense Distributed Files.

A major constitutional problem with the ITAR scheme is that its definition of “export” prohibits general publication, public discussion, and scientific and academic exchange. *See* 22 C.F.R. § 120.17(a)(4). The government cannot censor these protected speech activities merely by relabeling them as the “conduct” of export. The regime is manifestly a direct regulation of expression, not mere conduct.

ITAR criminalizes the publication of “information in the form of blueprints, drawings, photographs, plans, instructions or documentation” or software, when that information relates to any of the wide range of technologies on the United States Munitions List. 22 C.F.R. § 120.10(a). Like paper documentation and blueprints, the digital documentation and design files such as Computer-Aided Design (CAD) files are speech that benefits from the full protection of the First Amendment. The government will be unable to establish otherwise. *See Freedman v. Maryland*, 380 U.S. 51, 58 (1965) (“the burden of proving that the film is unprotected expression must rest on the censor”).

A. Publishing Technical Information is Protected Speech.

It is settled that “the creation and dissemination of information are speech within the meaning of the First Amendment.” *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011) (collecting cases). As the Supreme Court has explained, “if the

acts of ‘disclosing’ and ‘publishing’ information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct.” *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001) (citation omitted). The expression of “‘all ideas having even the slightest redeeming social importance,’ including those concerning ‘the advancement of truth, science, morality, and arts’ have *the full protection* of the First Amendment.” *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000) (quoting *Roth v. United States*, 354 U.S. 476, 484 (1957)) (emphasis added).

This protection encompasses factual information such as technical data: “the First Amendment protects scientific expression and debate just as it protects political and artistic expression.” *Bd. of Trs. of Leland Stanford Jr. Univ. v. Sullivan*, 773 F. Supp. 472, 474 (D.D.C. 1991). “Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs.” *Sorrell*, 131 S. Ct. at 2667. And “[t]he purpose of the free speech clause . . . is to protect the market in ideas, broadly understood as the public expression of ideas, narratives, concepts, imagery, opinions—scientific, political or aesthetic.” *Dambrot v. Cent. Mich. Univ.*, 55 F.3d 1177, 1188 (6th Cir. 1995) (alterations in original) (quoting *Swank v. Smart*, 898 F.2d 1247, 1250 (7th Cir. 1990)).

Even instructions on how to conduct potentially dangerous activities are protected speech. *Herceg v. Hustler Magazine, Inc.*, 814 F.2d 1017, 1019 (5th Cir. 1987). In *Herceg*, this Court held that the First Amendment shielded Hustler Magazine from liability for the death of a young man who engaged in “autoerotic asphyxiation” after reading how to do it in the magazine. *Id.* The Court explained that “first amendment protection is not eliminated simply because publication of an idea creates a potential hazard.” *Id.* at 1020; accord *Winter v. G.P. Putnam’s Sons*, 938 F.2d 1033, 1034 (9th Cir. 1991) (publisher not liable for illness from eating mushrooms described in its *Encyclopedia of Mushrooms*).

The Supreme Court explained in *Bartnicki* that “it would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party.” 532 U.S. at 529-30. After all, “[m]uch speech is dangerous. Chemists whose work might help someone build a bomb, political theorists whose papers might start political movements that lead to riots, speakers whose ideas attract violent protesters, all these and more leave loss in their wake.” *Am. Booksellers Ass’n. v. Hudnut*, 771 F.2d 323, 333 (7th Cir. 1985), *aff’d mem.*, 475 U.S. 1001 (1986), *reh’g denied*, 475 U.S. 1132 (1986). Yet “[t]he prospect of crime..., by itself does not justify laws suppressing protected speech.” *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 245 (2002).

B. Computer-Readable Documentation and Designs, Like Those of Defense Distributed, Are Protected Speech.

Defense Distributed's design files exemplify the protected speech burdened by ITAR's ban on Internet publication. They are informational documents that directly communicate technical ideas such as the dimensions and specifications of objects. *See* ROA.335-36.

The files fall into two main categories: general documentation and Computer-Aided Design (CAD) files. ROA.335-36. The first category includes traditional media such as image files and Microsoft Word documents describing objects. *Id.* Visual and written descriptions are traditional formats for protected expression. *E.g., Kaplan v. California*, 413 U.S. 115, 119–120 (1973) (explaining that photographs, like printed materials, are protected by the First Amendment). ITAR clearly burdens protected speech by prohibiting the disclosure of “blueprints, drawings, photographs, plans, instructions or documentation.” 22 C.F.R. § 120.10(a)(1).

The other, equally-protected, category of documents at issue here consists of CAD files. *See* ROA.335-36 (describing four CAD file formats). CAD files are specifications describing the shape and sometimes the physical makeup of three-dimensional objects. A CAD file might describe a solid cube by specifying its corners as coordinates in three dimensions: (0, 0, 0); (0, 1, 0); (1, 1, 0); and so on.

In the common .stl CAD language, the definition of this “solid cube” would begin as follows and repeat until each facet of the shape is defined:³

```
solid cube  
facet normal 0 0 0  
outer loop  
vertex 0 0 0  
vertex 0 1 0  
vertex 1 1 0  
endloop  
endfacet
```

More elaborate .stl shapes, such as the Statue of Liberty⁴ or a firearm, are described the same way: listing coordinates that define the object’s surface.⁵

To create a physical object based on a CAD file, a third party must supply additional software to read these files and translate them into the motions of a 3D print head,⁶ the 3D printer itself, and the necessary physical materials.

The government incorrectly argues that technical data files lose First Amendment protection because of their “function.” Defs.’ Opp’n Prelim. Inj. 16. However, “[t]he fact that a medium of expression has a functional capacity should

³ See Solid Cube, <http://cpansearch.perl.org/src/EWILHELM/CAD-Format-STL-v0.2.1/files/cube.stl>.

⁴ hroncok, *Statue of Liberty with Base Building*, Thingiverse (Mar. 25, 2013), <http://www.thingiverse.com/thing:65869/#files>.

⁵ Wai Hon Wah, *Introduction to STL format*, (June 1999) http://download.novedge.com/Brands/FPS/Documents/Introduction_To_STL_File_Format.pdf

⁶ Slic3r Home Page, <http://slic3r.org/> (last visited Dec. 15, 2015) (“Slic3r is the tool you need to convert a digital 3D model into printing instructions for your 3D printer. It cuts the model into horizontal slices (layers), generates toolpaths to fill them and calculates the amount of material to be extruded.”)

not preclude constitutional protection.” *Junger v. Daley*, 209 F.3d 481, 484-85 (6th Cir. 2000) (discussing computer source code); see *Bernstein v. U.S. Dep’t of State*, 922 F. Supp. 1426, 1435-36 (N.D. Cal. 1996) (same). Computer software consistently receives First Amendment protection because code, like a written musical score, “is an expressive means for the exchange of information and ideas.” *Junger*, 209 F.3d at 485; see *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001) (decryption software). The functional consequences of speech are considered not as a bar to protection, but to whether a regulation burdening the speech is appropriately tailored. *Junger*, 209 F.3d at 485.

Further, ITAR does not restrict itself to executable computer software that some courts have described as “functional” (and which they have *protected* nonetheless). The design files at issue here, for example, are not “functional” software that can be “run,” “launched,” or “executed.” They are storage files for text, images, and three-dimensional shapes, having “functional” consequences only after a third party interprets and implements them with software, hardware (such as a 3D printer), and raw materials. Even under the government’s flawed view that “functionality” diminishes First Amendment protection, files here are, if anything, less “functional,” and at least as protected, as the computer instructions for encrypting data at issue in *Bernstein* and *Junger* or the decryption instructions at issue in *Corley*.

C. First Amendment Protection is Not Diminished For Speech That is Accessible to Foreigners.

The Ninth Circuit, in *Bullfrog Films, Inc. v. Wick*, invalidated regulations regarding the export of educational, scientific, and cultural materials as being facially inconsistent with the First Amendment, overly broad, and vague. 847 F.2d 502, 509-14 (9th Cir. 1988). The court held that “the First Amendment protects communications with foreign audiences to the same extent as communication within our borders.” *Id.* at 509 n.9, 511-512 (declining to revisit this “well-reasoned conclusion” of the district court, which further explained that “there is no ‘sliding scale’ of First Amendment protection under which the degree of scrutiny fluctuates in accordance with the degree to which the regulation touches on foreign affairs. Rather, the only permissible non-neutral inquiry into the content of the speech is whether the statements adversely affect foreign policy interests to such a degree that the speech is completely unprotected.” *Bullfrog Films, Inc. v. Wick*, 646 F. Supp. 492, 502-04 (C.D. Cal. 1986)). Besides, ITAR burdens speech to a foreigner within the United States. 22 C.F.R. § 120.17(a)(4). With the rise of the Internet, it is all the more crucial that the free speech rights of Americans are not diminished merely because online speech is accessible to foreigners.

In sum, ITAR burdens protected speech, including the design files at issue in this case. Only under an appropriately-tailored regime with adequate First

Amendment safeguards could the government restrict the publication of such information.

III. ITAR’s Prepublication Review of Technical Data Is an Unlawful Prior Restraint on Speech.

A. Speech-Licensing Regimes that Lack Procedural Safeguards are Invalid.

Licensing schemes that create a system of pre-publication review for protected speech are unconstitutional unless the review process is bounded by stringent procedural safeguards. *Freedman v. Maryland*, 380 U.S. 51, 58–59 (1965). A scheme making the “freedoms which the Constitution guarantees contingent upon the uncontrolled will of an official—as by requiring a permit or license which may be granted or withheld in the discretion of such official—is an unconstitutional censorship or prior restraint upon the enjoyment of those freedoms.” *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 226 (1990) (plurality opinion) (quoting *Shuttlesworth v. Birmingham*, 395 U.S. 147, 151 (1969)); *see also Se. Promotions, Ltd. v. Conrad*, 420 U.S. 546, 553 (1975). Human nature creates an unacceptably high risk that excessive discretion will be used unconstitutionally, and such violations would be very difficult to prove on a case-by-case basis. *Lakewood v. Plain Dealer Pub. Co.*, 486 U.S. 750, 758 (1988). Furthermore, “[b]ecause the censor’s business is to censor, there inheres the danger that he may well be less responsive than a court—part of an independent branch of

government—to the constitutionally protected interests in free expression.”
Freedman, 380 U.S. at 57-58.

A regulation “subjecting the exercise of First Amendment freedoms to the prior restraint of a license, without narrow, objective, and definite standards to guide the licensing authority, is unconstitutional.” *Shuttlesworth v. City of Birmingham, Ala.*, 394 U.S. 147, 150-51 (1969); accord *Lakewood*, 486 U.S. at 770-72. The Supreme Court warned in *Lakewood*, where a license could be denied for not being in the “public interest,” that “[t]o allow these illusory ‘constraints’ to constitute the standards necessary to bound a licensor’s discretion renders the guaranty against censorship little more than a high-sounding ideal.” *Lakewood*, 486 U.S. at 769-70; see also *Bernstein v. U.S. Dep’t of State*, 974 F. Supp. 1288, 1308 (N.D. Cal. 1997) (holding that “national security and foreign policy interests” are “illusory constraints”).

Speech licensing schemes are also invalid when they lack certain procedural protections:

- 1) the licensing decision must be prompt;
- 2) there must be prompt judicial review; and
- 3) when a censor denies a license, it must go to court to obtain a valid gag order and once there bears the burden to prove the gag is justified.

See *Freedman*, 380 U.S. at 58-60.

As the Supreme Court has explained, “because only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint.” *Id.* at 58. “Any restraint imposed in advance of a final judicial determination on the merits must similarly be limited to preservation of the status quo for the shortest fixed period compatible with sound judicial resolution. . . . [T]he procedure must also assure a prompt final judicial decision, to minimize the deterrent effect of an interim and possibly erroneous denial of a license.” *Id.* at 59. Even a court-ordered prior restraint on speech must be stayed if appellate review is not expedited. *Nat. Socialist Party of Am. v. Skokie*, 432 U.S. 43, 43-44 (1977) (per curiam). The Court has not specified precisely when a final judicial decision must come, but it must be faster than the four months for initial judicial review and six months for appellate review in *Freedman*, 380 U.S. at 55, 61. The regime it cited with approval required “a hearing one day after joinder of issue; the judge must hand down his decision within two days after.” *Id.* at 60.

Even content-neutral licensing schemes are unconstitutional if they lack these safeguards. *Lakewood*, 486 U.S. at 763-64; *see FW/PBS*, 493 U.S. at 227 (plurality opinion) (city did not pass judgment on content of protected speech, but impermissibly had indefinite amount of time to issue license). Licensing schemes create a heightened risk of discriminatory application; the newsrack permitting

scheme in *Lakewood* was neither facially content-based nor justified in terms of content, but it was still struck down because it could be applied discriminatorily. *Lakewood*, 486 U.S. at 757-59.

B. ITAR’s Prepublication Review Scheme Lacks the Required Safeguards.

The prepublication review process lacks *every single one* of the required safeguards. *See Bernstein v. U.S. Dep’t of State*, 945 F. Supp. 1279, 1289 (N.D. Cal. 1996) (“The ITAR scheme, a paradigm of standardless discretion, fails on every count.”).

First, the regulatory scheme fails to provide binding standards. A license may be denied whenever the Department of State deems it “advisable.” 22 C.F.R. § 126.7(a)(1). The regime is even more egregious than those that purport to be bounded by “illusory constraints,” *Lakewood*, 486 U.S. at 769, such as “national security and foreign policy interests.” *Bernstein*, 974 F. Supp. at 1307. It is even more vague than the one rejected by this Court in *Fernandes v. Limmer*, where the agency could refuse permission to speak “when there is good reason to believe that the granting of the permit will result in a direct and immediate danger or hazard to the public security, health, safety or welfare.” 663 F.2d 619, 631 (5th Cir. 1981). Rather than putting the public on notice of what is prohibited, ITAR’s prepublication review regime invites the public to ask on a case-by-case basis and reserves the right to deny a license at the pleasure of the agency.

Second, the scheme does not guarantee prompt adjudication. There are no binding deadlines for adjudication of a commodity jurisdiction request, and while Presidential guidance requires that license applications be adjudicated within 60 days, the deadline is swallowed by broad exemptions and does not require that administrative appeals adhere to any deadline. Policy on Review Time for License Applications, 74 Fed. Reg. 63,497 (Dec. 3, 2009); *see* 22 C.F.R. § 126.7(c). Here, a commodity jurisdiction decision took nearly two years. App. Br. 23.

Third, the ITAR regime fails to provide for prompt judicial review of licensing determinations: because an ITAR determination “is highly discretionary, it is excluded from review under the Administrative Procedure Act.” 22 C.F.R. § 128.1. The complete lack of judicial safeguards means that the ITAR speech-licensing scheme cannot satisfy *Freedman’s* requirements that such a regime provide for prompt judicial review and “that the licensor will, within a specified brief period, either issue a license or go to court.” *Riley v. Nat’l Fed’n of Blind of N.C., Inc.*, 487 U.S. 781, 802 (1988) (*quoting Freedman*, 380 U.S. at 59). The executive branch may not create a speech-licensing regime independent of judicial checks and balances.

C. The Government Incorrectly Argues that ITAR Prepublication Review is Not a Prior Restraint.

The government attempts to characterize the prepublication review requirement as something other than a prior restraint. It relies on two Ninth Circuit

cases that considered the lawfulness of export controls. *United States v. Chi Mak*, 683 F.3d 1126 (9th Cir. 2012); *United States v. Edler Indus., Inc.*, 579 F.2d 516, 521 (9th Cir. 1978). Yet until very recently, the government had disavowed the prepublication review requirement, giving those panels no occasion to consider it. ROA.332 (“Approval is not required for publication of data within the United States as described in Section 125.11(a)(1). Footnote 3 to Section 125.11 does not establish a prepublication review requirement.”). The government also had not asserted that the “public domain” exception of § 120.11(a) excludes publication on the Internet, now the nation’s dominant medium for speech. In *Chi Mak*, the court relied on that public domain exception to protect “the types of information that are subject to the highest levels of First Amendment protection.” 683 F.3d at 1136. *Edler* also predated the provisions eliminating judicial review for ITAR and the bulk of Supreme Court caselaw elaborating *Freedman*. 22 C.F.R. § 128.1 (effective Sept. 17, 1996); 22 U.S.C. § 2778(h). Further, it adopted a narrowing construction that is not clearly reflected in the statute: rather than *Edler*’s specific knowledge requirement, the statute merely requires that violations be willful. *Compare* 22 U.S.C. § 2778(c) *with Edler*, 579 F.2d at 521.

Whatever an appropriately-tailored export control regime may be, it cannot involve, as here, a broad prior restraint against Internet publication, subject to unbounded agency discretion lacking any judicial review. The Court should

conclude on this basis alone that plaintiff-appellants are likely to prevail on their First Amendment claim.

IV. The Government Cannot Show that the Speech Burdened by Prepublication Review Would Cause Direct, Immediate, and Irreparable Harm to National Security.

The Supreme Court has repeatedly held that prior restraints may be sustained only in extraordinary circumstances: prior restraints must be strictly *necessary* to further a governmental interest of the highest magnitude. *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 562 (1975); *accord CBS Inc. v. Davis*, 510 U.S. 1315, 1317 (1994) (“Even where questions of allegedly urgent national security or competing constitutional interests are concerned . . . we have imposed this most extraordinary remedy only where the evil that would result from the reportage is both great and certain and cannot be mitigated by less intrusive measures.”) (quotations and citations omitted).

A prior restraint is considered justifiable only if: (1) the harm to the governmental interest will definitely occur; (2) the harm will be irreparable; (3) no alternative exists for preventing the harm; and (4) the prior restraint will actually prevent the harm. *Nebraska Press*, 427 U.S. at 562.

This exacting scrutiny applies even if the asserted governmental interest is national security. In the *Pentagon Papers* case, *N.Y. Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam), the Supreme Court the government failed to

carry the “heavy burden of showing justification for the imposition of [] a restraint” against publishing a classified report on Vietnam. 403 U.S. at 714. The narrowest concurrence⁷ rejected the prior restraint because the Justices “[could not] say that disclosure of any of [the documents] will surely result in direct, immediate, and irreparable damage to our Nation or its people.” 403 U.S. at 730 (Stewart, J., concurring); *see Fernandes*, 663 F.2d at 631 (adopting “direct, immediate, and irreparable damage” standard of the Stewart concurrence).

ITAR’s prepublication review scheme cannot satisfy these requirements. Here, prior restraint is imposed without any showing of harm, let alone the required showing that disclosure will “surely result” in “direct, immediate, and irreparable damage.” *Pentagon Papers*, 403 U.S. at 730 (Stewart, J., concurring). A prior restraint that operates in the absence of proven harm fails the *Nebraska Press* requirements of “the requisite degree of certainty to justify the restraint,” that there be no alternative measures, and that the restraint “effectively . . . operate to prevent the threatened danger.” 427 U.S. at 569-70, 562.

The regime here also makes no effort to tailor restrictions to individual, case-by-case circumstances. The ban categorically forbids online speech about

⁷ The “narrowest grounds” for concurring are regarded as the Court’s holding. *See Marks v. United States*, 430 U.S. 188, 193 (1977).; *see also Fernandes v. Limmer*, 663 F.2d 619, 631 (5th Cir. 1981).

science and technologies that potentially implicate ITAR, whether or not specific speech poses a particular risk.

The government merely argues that the designs here “could be used” to create and use a weapon against U.S. interests. Defs.’ Opp’n Prelim. Inj. 10. This falls far short of the required showing under *Nebraska Press*. Even if the designs did communicate information that “could be used” in a harmful way, the government has not demonstrated that prior restraint is so strictly necessary to a concrete, critical interest that the First Amendment will allow it.

V. ITAR’S Ban on Publications IS a Content-Based Regulation that Fails Strict Scrutiny.

Independent of its defects as a prior restraint, the prepublication review scheme fails to satisfy the strict First Amendment scrutiny required of restrictions on content. *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2664 (2011). Because the government cannot show the regulations are narrowly tailored to advance a compelling state interest, they cannot permissibly be enforced in the overbroad manner it urges.

A. ITAR Is a Content-Based Regulation of Speech.

ITAR regulations are triggered by the topic of speech, namely the communication of information about technologies governed by ITAR. The Supreme Court recently reiterated that “defining regulated speech by particular subject matter” is an “obvious” content-based regulation. *Reed v. Town of Gilbert*,

135 S. Ct. 2218, 2227 (2015). More “subtle” content-based distinctions involve “defining regulated speech by its *function or purpose*.” *Id.* (emphasis added). And it has long been recognized that “the First Amendment’s hostility to content based regulation extends not only to a restriction on a particular viewpoint, but also to a prohibition of public discussion of an entire topic.” *Burson v. Freeman*, 504 U.S. 191, 197 (1992); accord *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 116 (1991) (statute restricting speech about crime is content-based); *Consolidated Edison Co. of N.Y. v. Public Service Comm’n of N.Y.*, 447 U.S. 530, 537-38 (1980).

A regulation that involves a licensor in appraising facts, exercising judgment, and forming opinions is also a content-driven scheme. See, e.g., *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 135-36 (1992) (permit fee based on the capacity for a march to cause violence was content-based); *Cantwell v. Connecticut*, 310 U.S. 296, 305 (1940) (censor asked to determine whether a cause is “religious”).

In ITAR’s prepublication review scheme, regulation of speech is triggered when it describes covered subject matter. In both the commodity jurisdiction and licensing processes, the government analyzes the content of the particular speech to decide whether it discusses subject matter that should be controlled under ITAR, judge its communicative impact, and determine whether blocking the disclosure is

“in furtherance of world peace, the national security or the foreign policy of the United States, or is otherwise advisable.” 22 C.F.R. § 126.7. Just like the regulators in *Forsyth County*, who evaluated the capacity of a message to lead to violence, ITAR regulators are engaged in the content-based regulation of speech when they make individualized censorship decisions.

The government argues that a “content-neutral purpose” underlies the regulations, but that is irrelevant here.⁸ Defs.’ Opp’n Prelim. Inj. 15-16. “A law that is content based on its face is subject to strict scrutiny regardless of the government’s benign motive, content-neutral justification, or lack of ‘animus toward the ideas contained’ in the regulated speech.” *Reed*, 135 S. Ct. at 2228 (quoting *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 429 (1993)). The government here has chosen content-based *means* to achieve its purpose, requiring strict scrutiny. *See Lakewood*, 486 U.S. at 759 (striking down a newsrack ordinance because of censorial effects, without discussing governmental purpose for enacting the ordinance); *see also Minneapolis Star & Tribune Co. v. Minnesota Comm’r of Revenue*, 460 U.S. 575, 592 (1983) (illicit legislative intent is not necessary for a First Amendment violation); *Cantwell*, 310 U.S. at 304-05 (assuming a proper purpose, “the question remains whether the method adopted by Connecticut to that end transgresses the liberty safeguarded by the Constitution”).

⁸ Besides, preventing the spread of information on certain topics is hardly “content-neutral.”

B. ITAR Does Not Satisfy Strict Scrutiny.

The government bears the burden of showing that the regulations are necessary to serve a compelling state interest and are narrowly tailored to serve that interest. *U.S. v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000). A regulation is not narrowly tailored if:

- it fails to advance the relevant interest,⁹
- it burdens substantially more speech than is necessary to vindicate the interest,¹⁰
- less-restrictive means were available to achieve the same ends,¹¹ or
- it is underinclusive and thus burdens speech without advancing the asserted interest.¹²

Just as “the Government may not reduce the adult population to only what is fit for children,” *Reno v. ACLU*, 521 U.S. 844, 875 (1997), neither may it reduce the online speech of Americans to only what is fit for foreign consumption.

⁹ See, e.g., *Eu v. San Francisco County Democratic Cent. Committee*, 489 U.S. 214, 226, 228-29 (1989); *Meyer v. Grant*, 486 U.S. 414, 426 (1988); *Globe Newspaper Co. v. Superior Court for Norfolk*, 457 U.S. 596, 609-10 (1982); *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 789-90 (1978); *Buckley v. Valeo*, 424 U.S. 1, 45-47, 53 (1976).

¹⁰ See, e.g., *Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.*, 502 U.S. 105, 120-21 (1991); *FEC v. Nat'l Conservative Political Action Comm.*, 470 U.S. 480, 500-01 (1985).

¹¹ *U.S. v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000); *R. A. V. v. City of St. Paul*, 505 U.S. 377, 395 (1992); *FEC v. Mass. Citizens for Life, Inc.*, 479 U.S. 238, 262 (1986).

¹² *Florida Star v. B.J.F.*, 491 U.S. 524, 540 (1989).

Banning Internet publication prevents valuable domestic debate and sharing of information, and represents a radical departure from traditional export controls.

1. Less-Restrictive Means Are Available to Address ITAR's Goals.

The history of ITAR further demonstrates that prepublication review is not necessary to achieve the government's goals. In 1980, the State Department responded to First Amendment concerns by repudiating the existence of a prepublication review requirement: "Approval is not required for publication of data within the United States as described in Section 125.11(a)(1). Footnote 3 to section 125.11 does not establish a prepublication review requirement."¹³ The State Department revised the regulations several times to clarify that it was *not* purporting to impose an unconstitutional licensing regime, in response to concerns from the Department of Justice.¹⁴

ITAR has long recognized that it is inappropriate and unnecessary to constrain the publication of unclassified information into the public domain. *See* 22 C.F.R. § 120.11. Yet the government now takes the position that the Internet does not qualify as the "public domain." Defs.' Opp'n Prelim. Inj. 3 n.3.¹⁵ The arbitrary

¹³ U.S. Dep't of State, *Munitions Control Newsletter*, <https://app.box.com/s/ohqvn3b6tawz9d65g12s3ri2gpxo8fdp>.

¹⁴ *DOJ Memos on ITAR Prior Restraint*, Defense Trade Law Blog, July 9, 2015, <http://defensetradelaw.com/2015/07/09/doj-memos-on-itar-prior-restraint/>.

¹⁵ This position is contrary to the plain meaning of "public domain" and 22 C.F.R. § 120.11 (a)(4), which includes information available at public libraries. Among

distinction between electronic publication and other media is irrational and untenable. ITAR recognizes that the public domain includes information available “[a]t libraries open to the public or from which the public can obtain documents.” 22 C.F.R. § 120.11(a)(4). ITAR also defines the public domain to include publications sold at newsstands and bookstores and subscriptions that “are available without restriction to any individual who desires to obtain or purchase the published information.” *See* 22 C.F.R. §§ 120.11 (a)(1), (2). These media are freely available to foreign persons, and the exact same information could be published electronically or in print form. If these media need not be restricted to achieve the government’s ends, the entire medium of Internet publication need not be presumptively off-limits for communication about defense-related technologies.

A substantial body of law provides alternative means for securing sensitive defense information, including the government clearance system and contractual restraints on disclosure. These approaches reflect the traditional First Amendment

public libraries, 99% have public Internet connections, averaging nineteen computers per location. Information Policy & Access Center, 2014 Digital Inclusion Survey (2015), <http://digitalinclusion.umd.edu/sites/default/files/uploads/2014DigitalInclusionSurveyFinalRelease.pdf>. Americans consider Internet access at public libraries to be just as important as providing access to books. Kathryn Zickuhr, et al., *Library Services in the Digital Age*, Pew Internet, Jan. 22, 2013, <http://libraries.pewinternet.org/2013/01/22/part-4-what-people-want-from-their-libraries/>. The exception for subscriptions also applies: an Internet user can subscribe to the content of any website (many websites make this effortless with “feeds”). *See* 22 C.F.R. § 120.11(a)(2).

distinction between restraints on disclosure of information that one has a duty to keep secret as a result of a sensitive position or agreement, as opposed to information one has independently discovered or generated. *See United States v. Aguilar*, 515 U.S. 593, 606 (1995) (“Government officials in sensitive confidential positions may have special duties of nondisclosure.”). *Compare Boehner v. McDermott*, 484 F.3d 573, 579 (D.C. Cir. 2007) (en banc) (punishing disclosure of information obtained by defendant in his role as member of House Ethics Committee), *with Jean v. Mass. State Police*, 492 F.3d 24, 32 (1st Cir. 2007) (protecting similar disclosure, and noting that the court in *Boehner* would have done the same “if McDermott had been a private citizen, like Jean”).

Similarly, Congress considered (and rejected) changes to the Undetectable Firearms Act that would have addressed the creation, transport, or sale of any 3D printed firearm that was not detectable by standard means.¹⁶ This approach demonstrates that protected speech need not be burdened to vindicate a government interest in preventing the use of certain weaponry.

¹⁶ Kasie Hunt & Carrie Dann, *Senate Extends Ban on Undetectable Guns But Nixes Tighter Restrictions*, NBC News, Dec. 9, 2013, <http://www.nbcnews.com/news/other/senate-extends-ban-undetectable-guns-nixes-tighter-restrictions-f2D11717122>; Undetectable Firearms Modernization Act, H.R. 3643, 113th Cong. (2013); Undetectable Firearms Reauthorization Act, S.1774, 113th Cong (2013).

2. *Most Speech Burdened by ITAR Does Not Threaten Any Concrete Government Interest.*

The scope of ITAR's prohibition on speech could apply to members of the press republishing newsworthy technical data, professors educating the public on scientific and medical advances of public concern, enthusiasts sharing otherwise lawful information about firearms, domestic activists trading tips about how to treat tear gas or resist unlawful surveillance, and gun control opponents expressing a point about proliferation of weapons. Innocent online publication on certain topics is prohibited simply because a hostile foreign person could conceivably locate that information, use it to create something harmful, and use a harmful device against US interests. Speech cannot permissibly be repressed for such an attenuated and hypothetical government end.

Similarly, ITAR forbids the re-publication of information that is already available on the public Internet, because the government does not recognize the Internet as "public domain." Defs.' Opp'n Prelim. Inj. 3 n.3; *see* ROA.335-38. Banning this re-publication does not meaningfully advance any government interest: "punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act." *Florida Star v. B.J.F.*, 491 U.S. 524, 535 (1989).

3. *Alternative Channels for Speech Do Not Justify the Restraint.*

The government incorrectly asserts that the restraint on speech is justified because alternative channels of communication are left intact. Defs.’ Opp’n Prelim. Inj. 22. However, supposed alternative channels cannot overcome the challenged program’s content discrimination. As the Supreme Court explained in *Reno*:

This argument is unpersuasive because the CDA regulates speech on the basis of its content. A “time, place, and manner” analysis is therefore inapplicable. ... The Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books. In invalidating a number of laws that banned leafletting on the streets regardless of their content--we explained that “one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place.”

Reno, 521 U.S. at 879-80 (quoting *Schneider v. N.J. Twp. of Irvington*, 308 U.S. 147, 163 (1939)).

Furthermore, even if there were no content discrimination here, there *are* no adequate alternative channels of communication. There is no medium of expression that is equivalent to Internet publication, enabling Americans to engage with strangers and colleagues who agree or vehemently disagree with their views in real time from thousands of miles away—yet is inaccessible to foreigners. *See Reno*, 521 U.S. at 868-69 (describing the “vast democratic forums of the Internet”). Even if online platforms restricted themselves to domestic access, a user still could not speak freely because the regulations prohibit disclosure to foreign persons *in*

the United States. 22 C.F.R. § 120.17(a)(4). It would also be a trivial matter for any person abroad to obtain the information using commonly-available “virtual private network” services that pipe traffic through a computer located in the US. This is an overwhelmingly common practice among those who are frustrated by geo-blocking of media content or location-based discrimination.¹⁷ And regardless of the technology at issue, an overbroad regulation of speech simply cannot be justified by the theory that publishers could take on the burden of policing their readership to make sure they are not foreign; the Supreme Court explained in *Reno* the chilling effects that would result from such a regime. *Reno*, 521 U.S. at 865-67 (discussing access by minors).

The government will be unable to prove that the regulations at issue satisfy strict First Amendment scrutiny.

VI. The Prepublication Review Scheme Is Invalid Even Under the Reduced Scrutiny the Government Advocates.

Even if the prepublication review scheme were subject to intermediate scrutiny, the government “must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.” *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 664

¹⁷ See, e.g., Elise Dalley, *Bypassing Geo-blocked Sites*, Choice, Aug. 13, 2014, <https://www.choice.com.au/electronics-and-technology/internet/internet-privacy-and-safety/articles/bypass-geo-blocking>.

(1994). The regulation also may not “burden substantially more speech than is necessary to further the government's legitimate interests.” *Id.* at 665.

The tailoring requirement does not simply guard against an impermissible desire to censor. The government may attempt to suppress speech not only because it disagrees with the message being expressed, but also for mere convenience. Where certain speech is associated with particular problems, silencing the speech is sometimes the path of least resistance. But by demanding a close fit between ends and means, the tailoring requirement prevents the government from too readily sacrificing speech for efficiency.

McCullen v. Coakley, 134 S. Ct. 2518, 2534 (2014) (internal quotation omitted).

ITAR demonstrates exactly the preference for “mere convenience” that *McCullen* called out as impermissible. The overbreadth and poor tailoring discussed above are so egregious that the lesser standard of intermediate scrutiny cannot save the regime. The regulations sacrifice informed public debate and scientific learning, even where the disclosures at issue pose no threat to US interests. The government has done no more than “posit the existence of the disease sought to be cured” and assert that the regulations will cure it – not enough to carry its burden. *See Turner*, 512 U.S. at 664.

CONCLUSION

For the foregoing reasons, plaintiff-appellants are likely to prevail on their First Amendment claim.

Dated: December 17, 2015

Respectfully submitted,

By: /s/ Kit Walsh
Kit Walsh (CA SBN 303598)

ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
kit@eff.org

Counsel for Amicus Curiae

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME
LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE
REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C)**

I hereby certify as follows:

1. The foregoing Brief of *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B). The brief is printed in proportionally spaced 14-point type, and there are 6,999 words in the brief according to the word count of the word-processing system used to prepare the brief (excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii)).

2. The brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), and with the type style requirements of Fed. R. App. P. 32(a)(6). The brief has been prepared in a proportionally spaced typeface using Microsoft® Word for Mac 2011 in 14-point Times New Roman font.

Dated: December 17, 2015

/s/ Kit Walsh

Kit Walsh

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeal for the Fifth Circuit by using the appellate CM/ECF System on December 17, 2015. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: December 17, 2015

/s/ Kit Walsh _____
Kit Walsh

No. 15-50759

IN THE UNITED STATES COURT OF
APPEALS FOR THE FIFTH CIRCUIT

DEFENSE DISTRIBUTED; SECOND AMENDMENT FOUNDATION,
INCORPORATED

Plaintiffs - Appellants

v.

UNITED STATES DEPARTMENT OF STATE; JOHN F. KERRY, in His
Official Capacity as the Secretary of the Department of State; DIRECTORATE OF
DEFENSE TRADE CONTROLS, Department of State Bureau of Political Military
Affairs; KENNETH B. HANDELMAN, Individually and in his Official Capacity
as the Deputy Assistant Secretary of State for Defense Trade Controls in the
Bureau of Political-Military Affairs; C. EDWARD PEARTREE, individually and
in his Official Capacity as the Director of the Office of Defense Trade Controls
Policy Division; SARAH J. HEIDEMA, Individually and in her Official
Capacity as the Division Chief, Regulatory and Multilateral Affairs; Office of
Defense Trade Controls Policy; GLENN SMITH, Individually and in His Official
Capacity as the Senior Advisor, Office of Defense Trade Controls,

Defendants – Appellees

Appeal from the United States District Court
For the Western District of Texas, Austin Division
No. 15-cv-00372 (Hon. Robert Pitman)

**BRIEF OF REPRESENTATIVE THOMAS MASSIE AND CERTAIN
MEMBERS OF THE U.S. HOUSE OF REPRESENTATIVES AS AMICI
CURIAE IN SUPPORT OF APPELLANTS**

Raffi Melkonian
WRIGHT & CLOSE, LLP
One Riverway, Ste. 2200
Houston, Texas 77056
713-572-4321
713-572-4320 (fax)

**SUPPLEMENTAL CERTIFICATE
OF INTERESTED PERSONS**

Pursuant to Fifth Circuit Rule 29.2, I hereby certify that I am aware of no persons or entities, in addition to those listed in Appellants' brief, that have a financial interest in the outcome of this litigation. All amici are individuals.

TABLE OF CONTENTS

	Page
INTEREST OF AMICI	7
PRELIMINARY STATEMENT AND SUMMARY OF ARGUMENT	8
I. Congress did not delegate the power to ban the publication of lawful speech when it passed the Arms Export Control Act to regulate exports and imports of arms.	10
A. An Administrative Agency has only the power granted to it by Congress.....	10
B. Congress did not grant the State Department authority to regulate domestic, public speech when it passed the AECA.....	12
II. If the AECA has the effect the Government claims, then it would exceed Congress’ limited and enumerated powers.	18
III. Interpreting the AECA in the way the State Department demands would chill technological innovation.	22
CONCLUSION	24
CERTIFICATE OF SERVICE	26
CERTIFICATE OF COMPLIANCE.....	26
ECF CERTIFICATION	27

TABLE OF AUTHORITIES

	Page
Cases	
<i>Adams Fruit Co. v. Barrett</i> , 494 U.S. 638 (1990)	11
<i>Bernstein v. U.S. Dep’t of State</i> , 922 F. Supp. 1426 (N.D. Cal. 1996)	16
<i>Bernstein v. U.S. Dep’t of State</i> , 945 F. Supp. 1279 (N.D. Cal. 1996)	17
<i>Bond v. United States</i> , 131 S. Ct. 2355 (2011)	14, 21
<i>FDA v. Brown & Williamson Tobacco Corp.</i> , 529 U.S. 120 (2000)	16
<i>Long Island Care at Home, Ltd. v. Coke</i> , 551 U.S. 158 (2007)	11
<i>Louisiana Public Serv. Comm’n v. FCC</i> , 476 U.S. 355 (1986)	11
<i>MCI Telecommc’ns Corp. v. AT&T Co.</i> , 512 U.S. 218 (1994)	16
<i>National Federation of Independent Business v. Sebelius</i> , 132 S. Ct. 2566 (2012)	19
<i>New York Times v. United States</i> , 443 U.S. 713 (1971)	21
<i>New York v. United States</i> , 505 U.S. 144 (1992)	21
<i>NFIB v. Sebelius</i> , 132 S. Ct. 2566, 2646 (2012)	20

<i>Samora v. United States</i> , 406 F.2d 1095 (5th Cir. 1969).....	14
<i>Swan v. Finch Co. v. U.S.</i> , 190 U.S. 143 (1903)	13
<i>Texas Dep’t of Housing and Community Affairs v. Inclusive Communities Project, Inc.</i> , 135 S. Ct. 2507 (2015)	11
<i>U.S. v. 1903 Obscene Magazines, Customs Seizure</i> , 907 F.2d 1338 (2d Cir. 1990).....	13
<i>U.S. v. Dien Duc Huynh</i> , 246 F.3d 734 (5th Cir. 2001).....	13
<i>U.S. v. Ehsan</i> , 163 F.3d 855 (4th Cir. 1998).....	13
<i>U.S. v. Gregg</i> , 829 F.2d 1430 (8th Cir. 1987).....	14
<i>U.S. v. Lee</i> , 183 F.3d 1029 (9th Cir. 1999).....	14
<i>U.S. v. Mead Corp.</i> , 533 U.S. 218 (2001)	10
<i>U.S. v. Swarovski</i> , 592 F.2d 131 (2d Cir. 1979).....	14
<i>United States v. Van Hee</i> , 531 F.3d 352 6th Cir. 1976)	15
<i>United States v. Clark</i> , 435 F.3d 1100 (9th Cir. 2006).....	20
<i>United States v. Comstock</i> , 130 S. Ct. 1949 (2010)	19
<i>United States v. Edler Industries</i> , 579 F.2d 516 (9th Cir. 1978).....	15

<i>United States v. Morrison</i> , 529 U.S. 598 (2000)	19
<i>Whitman v. American Trucking Assns., Inc.</i> , 531 U.S. 457, 468 (2001).....	11

Statutes

22 U.S.C. § 2751	20
22 U.S.C. § 2778	12, 20
U.S. Const. Art. I §8.....	19, 20

INTEREST OF AMICI

Amici are current Members of the House of Representatives whose names are listed in the Appendix. Members of Congress have a particular interest in seeing that federal statutes are properly interpreted and implemented. Moreover, Members of Congress are bound by oath to support and defend the Constitution. Thus, this Court’s interpretation of the First, Second and Fifth Amendments—as well as this Court’s decisions construing the reach of the foreign commerce clause—are at the core of Amici’s duties and responsibilities.

Representative Thomas Massie, of Kentucky—an MIT-trained engineer and inventor—is a Member of the Committee on Science, Space & Technology. His views are particularly relevant because the State Department’s improper and unconstitutional interpretation of federal law is likely to chill scientific and technological advancement in the United States.

No party or counsel for a party authored or paid for this brief in whole or in part, or made a monetary contribution to fund the brief’s preparation or submission. All parties have consented to the filing of this brief.

PRELIMINARY STATEMENT AND SUMMARY OF ARGUMENT

This case can be resolved, as Appellants state, on constitutional grounds. Appellees' decision to impose a prior restraint on the mere publication of unclassified public speech in the United States violates the First, Second, and Fifth Amendments to the United States Constitution, for all the reasons set forth in Appellants' brief. Amici would be entirely satisfied with such a ruling.

Amici—who are duty-bound to preserve and defend the Constitution and ensure the Executive's adherence to statute—write to emphasize two additional points. First, even if Congress was empowered to pass a statute regulating domestic, public, speech through the foreign commerce clause, which is doubtful, the AECA is *not* that statute. The State Department's expansive interpretation of the AECA to permit regulating the online publication of unclassified public speech departs entirely from the statutory text and is due no deference whatsoever. Indeed, the Department of Justice has long rejected the very reading the State Department adheres to now.

Second, it is doubtful that the AECA, which was promulgated by Congress under the foreign commerce clause to regulate foreign commerce, can constitutionally be applied to purely domestic publication. The federal government is a government of limited, enumerated powers, set within a federalist framework.

Appellees' conception of the AECA permits the foreign commerce clause to reach deep into the United States to regulate domestic public speech.

To be sure, Amici understand the State Department's duty to protect national security. That is a valid concern in this time of numerous foreign threats. But even if Appellants' speech constituted some kind of risk to national security, which Appellants amply demonstrate it does not, the solution to that problem is not to stretch the meaning of a clear statute to the breaking point or to violate the Constitution's limitations on federal power. Congress is the actor that can pass common sense legislation to foster the growth of an important technology while also protecting national security. The State Department should work with Congress to pass new legislation, if necessary, rather than unilaterally breaking the bounds of a Cold War-era statute.

Simply put, the State Department has violated Appellants' rights, and it has done so by trampling on the plain meaning of the AECA and on the wise restrictions imposed on the federal government by the Framers. The judgment below should be reversed.

ARGUMENT

I. Congress did not delegate the power to ban the publication of lawful speech when it passed the Arms Export Control Act to regulate exports and imports of arms.

Even assuming that Congress has the theoretical power to ban domestic speech through a law designed to control the import and export of defense articles—which it does not for the reasons set forth in Part II, *infra*—it has not done so. The State Department’s interpretation of the Arms Export Control Act permitting such regulation through the International Traffic in Arms Regulations (“ITAR”) is inconsistent with the text of the AECA, inconsistent with the AECA’s legislative history and purpose, and is inconsistent with the way the Department of Justice itself has interpreted and litigated the AECA in the past. This is not a question of due deference to an administrative agency: the State Department’s interpretation boldly (and impermissibly) departs from Congress’s intent to the detriment of all Americans’ First, Second, and Fifth Amendment rights. The district court adopted the Executive’s argument wholesale in its judgment. It cannot be upheld.

A. An Administrative Agency has only the power granted to it by Congress.

This case is not about deference to the State Department. It is about the very power of that agency to act in the way that it has, a core question of law entrusted to the courts. *See U.S. v. Mead Corp.*, 533 U.S. 218, 233 (2001) (question is

“beyond the *Chevron* pale”). The question here is whether Congress has delegated to the State Department the power to impose a ban against the otherwise lawful online publication of unclassified data. In the absence of such delegation, the State Department “literally has no power to act.” *See Louisiana Public Serv. Comm’n v. FCC*, 476 U.S. 355, 374 (1986). Or, as the Supreme Court has explained, “[a] precondition to deference under *Chevron* is a congressional delegation of administrative authority.” *Adams Fruit Co. v. Barrett*, 494 U.S. 638, 649 (1990). *See also Long Island Care at Home, Ltd. v. Coke*, 551 U.S. 158, 173 (2007) (“[T]he ultimate question is whether Congress would have intended, and expected, courts to treat an agency’s rule, regulation or application of a statute, or other agency action as within, or outside, its delegation to the agency of ‘gap-filling’ authority.”). Such power must be clearly granted. “Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms of ancillary provisions—it does not, one might say, hide elephants in mouse holes.” *Whitman v. American Trucking Assns., Inc.*, 531 U.S. 457, 468 (2001).

The proper form of analysis begins with the text of the statute, and asks whether the AECA permits the regulation of domestic public speech. *See Texas Dep’t of Housing and Community Affairs v. Inclusive Communities Project, Inc.*, 135 S. Ct. 2507, 2516 (2015) (rejecting Solicitor General’s reliance on *Chevron*

deference and instead deciding whether, “under a proper interpretation of the FHA, housing decisions with a disparate impact are prohibited”).

B. Congress did not grant the State Department authority to regulate domestic, public speech when it passed the AECA.

As both the Government and the court below agree, the only source of congressional authority for Defendants’ conduct is the AECA. But that statute says nothing about the regulation of domestic public speech. Rather, the statute authorizes the President, “[i]n furtherance of world peace and the security and foreign policy of the United States . . . to control the *import* and *export* of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services.” 22 U.S.C. § 2778(a)(1).

This straightforward statutory language does not permit the State Department to ban the domestic publication of unclassified public speech through its current expansive interpretation of the word “export” and application of ITAR.

First, the State Department’s actions clash directly with text of the AECA and particularly its exclusive application to “export” and “import.” The word “export” in particular, which is the entire basis of the State Department’s position, simply cannot be stretched to mean domestic publication with incidental receipt by foreign persons. Dictionaries uniformly cabin exportation to “the sending of commodities out of a country,” or a “severance of goods from [the] mass of things

belonging to [the] United States with [the] intention of uniting them to [the] mass of things belonging to some foreign country.” *U.S. v. Ehsan*, 163 F.3d 855, 858 (4th Cir. 1998) (collecting dictionary definitions). Common-law decisions too have observed that exportation “involves the transit of goods from one country to another for the purpose of trade.” *Id.* This Court, for example, has held (albeit in the context of the arms embargo against Iran, not in an AECA case) that “exportation occurs when the goods are shipped to another country with the intent that they will join the commerce of that country.” *U.S. v. Dien Duc Huynh*, 246 F.3d 734, 741 (5th Cir. 2001). And the Supreme Court, echoing the words of the Attorney General, has long ago held agreed that the “legal notion . . . of exportation is a severance of goods from the mass of things belonging to this country with an intention of uniting them to the mass of things belonging to some foreign country or another.” *Swan v. Finch Co. v. U.S.*, 190 U.S. 143, 145 (1903); *see also U.S. v. 1903 Obscene Magazines, Customs Seizure*, 907 F.2d 1338, 1342 (2d Cir. 1990) (discussing long history of the word import, all of which define importation as “bringing an article into a country from the outside”).

The State Department’s rule, however, captures purely domestic discussions between Americans *in* America simply because those discussions were undertaken by means of the internet rather than on paper, or orally, or by any other method. To interpret “export” to mean “publish on the internet to the general public” simply

does not comport with the common meaning of the word. As the Supreme Court held in *Bond v. United States*, “[s]aying that a person ‘used a chemical weapon’ conveys a very different idea than saying the person ‘used a chemical in a way that caused some harm.’” 134 S. Ct. 2077, 2090 (2014). Similarly, saying a person “‘exported’” arms conveys a very different meaning than saying that they “‘published legal information in the United States that might be accessed by people outside the United States.’”

Moreover, the State Department’s position clashes with courts’ repeated holdings that the purpose of the AECA—the conduct of foreign commerce and foreign policy—is clear and easy to understand. As this Court long ago held, the Mutual Security Act of 1954, AECA’s predecessor, was “‘directed to the conduct of international affairs.’” *See Samora v. United States*, 406 F.2d 1095 (5th Cir. 1969); *see also U.S. v. Lee*, 183 F.3d 1029 (9th Cir. 1999) (“The regulation at issue is directed to a relatively small group of sophisticated international businessmen”); *U.S. v. Gregg*, 829 F.2d 1430, 1437 (8th Cir. 1987) (“There is no unconstitutional vagueness [in the AECA]. It is as simple a matter as forbidding a passenger to ride on a train without a valid ticket”); *U.S. v. Swarovski*, 592 F.2d 131, 133 (2d Cir. 1979) (“We are dealing here with a regulation of limited scope aimed at a small and relatively sophisticated group of persons”) (interpreting prior legislation). A statute that has an obvious purpose, and survived vagueness challenges precisely

because it was easy to understand and applied to easily ascertainable business activities, cannot be now interpreted to mean something entirely different simply because the State Department perceives a phantom threat of arms proliferation through 3D printing.

United States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978), which the State Department insists justifies its position here, is far afield. In that case, there was no dispute whatsoever that the technical data at issue was *exported*. Defendants there provided (and admitted providing) direct technical assistance to foreign companies concerning technology used in missile manufacture. *Id.* at 518. The issue, rather, was to what extent the Mutual Security Act of 1954 could limit the export of non-classified materials with simultaneously military and civilian uses abroad. The *Edler* court construed ITAR’s reach narrowly to “control the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise.” *Id.* at 521. Similarly, the case on which the *Edler* court relied, *United States v. Van Hee*, 531 F.3d 352, 356 (6th Cir. 1976) involved the sale of plans to make amphibious military vehicles to Portugal—squarely in the heart of the AECA’s and the Mutual Security Act’s export restrictions. Congress does not delegate “decision[s] of . . . economic and political significance”—such as the applicability of a statute regulating the export of arms to foreigners to domestic speech—in “cryptic . . . fashion,” *FDA v. Brown & Williamson Tobacco Corp.*,

529 U.S. 120, 160 (2000) or through “subtle device[s],” *MCI Telecomm’s Corp. v. AT&T Co.*, 512 U.S. 218, 231 (1994).

The State Department’s basic misconception in this case is betrayed by a hypothetical it used below. Adopting Appellants’ theory, it warned, would allow scofflaws to skirt the AECA by “creating a digital model, sending that digital version abroad, and thereby enabling foreign recipients” to automatically create arms. This is fanciful. If a party intentionally created an automatically replicating model and purposefully sent it abroad in exchange for money, that might properly be captured by the AECA. What *actually* happened here is that an American organization published information in America, just as if it had put that information on television or in a book. That foreigners might look at it is irrelevant to a proper understanding of the State Department’s power to ban it under the existing statute.

It is telling that the State Department’s position today is starkly inconsistent with the Department of Justice’s consistent public and litigation statements that the AECA and ITAR do not cover domestic speech. Appellants’ brief describes these in full, *see, e.g.*, Appellants’ Br. at 39, but they are worth repeating because the State Department’s 180 degree pivot from its previous statements is so startling. The litigation position the Department of Justice took in *Bernstein v. U.S. Dep’t of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) (*Bernstein I*) and *Bernstein v. U.S. Dep’t*

of *State*, 945 F. Supp. 1279 (N.D. Cal. 1996) (*Bernstein II*) is particularly probative. In those cases, as Appellants carefully detail, the State Department affirmatively argued that it “does not seek to control the various means by which information is placed in the public domain” or “review scientific information to determine whether it may be offered for sale at newsstands and bookstores, through subscriptions, second-class mail, or made available at libraries, or distributed at a conference or seminar in the United States.” (Appellants’ Br. at 15). Yet, now, the State Department arrogates itself the power to deem all domestic speech that might be taken abroad to be exports subject to prior restraints. This is astonishing.¹

As Appellants also note, the Department of Justice has also consistently warned that the AECA and ITAR do not give the State Department limitless authority:

- On May 11, 1978, the Department of Justice issued a memorandum to the White House, titled “Constitutionality under the First Amendment of ITAR Restrictions on Public Cryptography.” That memo made clear DOJ’s “doubt” that

¹ The State Department claimed, below, that the legislative history of the Arms Export Control Act supports its reading of the statute because Congress expressed its view that “arms transfers cannot become an automatic, unregulated process.” See H.R. Rep. No. 94-1144, at 12 (1976), *reprinted in* 1976 U.S.C.C.A.N. 1378, 1388. Putting aside the point, for the moment, that an appeal to legislative history cannot alter the plain text of the statute, nothing in that House Report supports the State Department’s position. The cited section of the House Report concerned Congress’s role in deciding the propriety of future arms transfers—“because of the importance which arms transfers have for our own national security, such decisions should be understood by, and have the support of, the Congress and the American people”—not the scope of the term “export” or the reach of the AECA into domestic affairs.

Congress “intended that the President regulate noncommercial dissemination or information.” *See* Letter from John M. Harmon, Assistant Attorney General at the Office of Legal Counsel for the Department of Justice, to Dr. Frank Press, Senior Advisor to the President, at p. 4, n. 7.

- On July 1, 1981, the Department of Justice issued another memorandum, this time to the State Department Office of Munitions Control, regarding concerns with the State Department proposed revisions to ITAR. OLC stated that, given the deep constitutional concerns and the overbreadth of ITAR given the statutory context, “the best legal solution is for the Department of State, not the courts, to narrow the ITAR so as to make it less likely that they will apply to protected speech in constitutionally impermissible circumstances.” ROA.256.

- On July 1, 1981, the Department of Justice issued a memorandum noting its concern that ITAR could have “a number of unconstitutional applications.” *See* Department of Justice, *Constitutionality of the Proposed Revision of the International Traffic in Arms Regulations* (1981).

- In April 1997, DOJ issued a report discussing the availability of bombmaking information. This report made clear the real limits on the “publication of true, lawfully obtained information.” *See* Department of Justice, *Report on the Availability of Bombmaking* (1997). (ROA.287)

The State Department has stretched the AECA beyond its breaking point because it fears new technology. It does not have the authority to make that decision absent new Congressional action permitting it to do so.

II. If the AECA has the effect the Government claims, then it would exceed Congress’ limited and enumerated powers.

Even if the AECA can be read as authorizing the State Department to ban Appellants’ speech, such action is unconstitutional absent a close nexus to foreign commerce. That is so under the First, Second, and Fifth Amendments, as set forth in the Appellants’ brief; but it is also true because no enumerated power permits

Congress to pass legislation banning the domestic publication of information. The only constitutional basis for the AECA, the foreign commerce clause, does not and cannot reach entirely domestic activity.

The Federal government is a government of limited and enumerated powers. “With its careful enumeration of federal powers and explicit statement that all powers not granted to the Federal Government are reserved, the Constitution cannot realistically be interpreted as granting the Federal Government an unlimited license to regulate.” *United States v. Morrison*, 529 U.S. 598, 618 n.8 (2000). Because its powers are limited, Congress does not have the power to regulate domestic public speech unless a specific enumerated power so states. The police power “belongs to the States and the States alone.” *United States v. Comstock*, 130 S. Ct. 1949, 1967 (2010) (Kennedy, J. concurring).

The determinative question, then, is to identify *which* enumerated power was exercised in enacting the AECA, and to determine whether that enumerated power permits Congress to regulate domestic public speech. *See, e.g., National Federation of Independent Business v. Sebelius*, 132 S. Ct. 2566, 2577 (2012) (“If no enumerated power authorized Congress to pass a certain law, that law may not be enacted”); *Comstock*, 560 U.S. at 163 (Thomas, J., dissenting) (noting Government’s failure to identify the “specific enumerated power or powers” that were the constitutional predicate for statute at issue).

The AECA’s text and context give us the answer to the first of those questions. A statute’s reference to foreign commerce triggers the foreign commerce clause, which gives Congress a broad grant of power to “regulate Commerce with foreign Nations.” U.S. Const. art. I, § 8, cl. 3. For example, the Ninth Circuit has held that a reference to the phrase “travels in foreign commerce” unequivocally invoked the foreign commerce clause. *See, e.g., United States v. Clark*, 435 F.3d 1100, 1114 (9th Cir. 2006). The text of the AECA, which authorizes the President to “control the *import* and *export* of defense articles and defense services,” 22 U.S.C. § 2778, is a clear reference to foreign commerce. In addition, the structure of the statute supports its plain meaning. First, the AECA constitutes Chapter 39 of Title 22 (“*Foreign Relations and Intercourse*”) and is codified at 22 U.S.C. § 2751. Moreover, the prefatory sections of the AECA found at 22 USC § 2751 make clear the goals that Congress had in seeking to control the export of weapons in service of foreign policy. Namely, the goals and purposes found therein relate exclusively to “world peace” and foreign policy. The AECA is thus grounded exclusively in Congress’ foreign commerce power found in U.S. Const. Art. I §8.²

² The necessary and proper clause can provide no basis for the application of the AECA to domestic speech through the foreign commerce clause power. As a majority of the members of the Supreme Court have stated, “the Necessary and Proper Clause is exceeded not only when the congressional action directly violates the sovereignty of States but also when it violates the background principle of enumerated (and hence limited) federal power.” *NFIB v. Sebelius*, 132 S. Ct. 2566, 2646 (2012) (joint dissent); *accord id.*, at 2592 (Roberts, C.J.)

Nor could it be otherwise. The Government itself concedes that the AECA does not reach domestic speech delivered person-to-person, or domestic speech published in a book or newspaper. That is because the Constitution does not create a national police power. The basic “allocation of powers in our federal system preserves the integrity, dignity, and residual sovereignty of the States . . . in part, [as] an end in itself, to ensure that States function as political entities in their own right.” *Bond*, 131 S. Ct. at 2364. The Constitution also divides authority between federal and state governments for the protection of individuals.” *New York v. United States*, 505 U.S. 144, 181 (1992). “By denying any one government complete jurisdiction over all the concerns of public life, federalism protects the liberty of the individual from arbitrary power.” *Bond v. United States*, 131 S. Ct. 2355, 2364 (2011). Imagine, for example, an American giving a speech that, if the contents were distributed abroad, could aid a foreign enemy. Congress could not ban such speech by prior restraint even if a foreign agent happened to be standing in the public square listening intently. *See, e.g., New York Times v. United States*, 403 U.S. 713, 735 (1971). Such action is beyond any conceivable domestic power granted to the Government by the Constitution other than the vague inherent powers the Supreme Court rejected in the Pentagon Papers case.

But, fundamentally, exactly that far-reaching power is the power the State

(noting that the necessary and proper clause is “narrow in scope” and operates to permit laws that are “incidental” to the exercise of enumerated powers).

Department claims here. The State Department's chosen interpretation of the AECA—that publishing information domestically on an open forum like the internet is the equivalent of exporting products—would capture almost any domestic publication of supposedly controlled information. Nor would simply limiting the rule to publication on the internet limit the intrusion on the Constitution in any serious way. The internet is today the pervasive and dominant way of communicating information. Just as the Supreme Court would not countenance speech restrictions that would violate the First Amendment if they were limited to the internet, so too this Court should not permit a violation of limited nature of the government simply because the government imposes an arbitrary limit on its unlawful actions.

III. Interpreting the AECA in the way the State Department demands would chill technological innovation.

The United States should be a leader in 3D printing, a scientific innovation that has the potential to dramatically change the world and benefit the United States. In *The Economist's* words, 3D printing “may have as profound an impact on the world as the coming of the factory did. . . Just as nobody could have predicted the impact of the steam engine in 1750—or the printing press in 1450, or the transistor in 1950—it is impossible to foresee the long-term impact of 3D printing. But the technology is coming, and it is likely to disrupt every field it touches.” Leaders, *Print me a Stradivarius*, *THE ECONOMIST*, February 2011.

3D printing is disruptive because it fundamentally changes how goods are manufactured. For example, rather than importing parts from far away, goods may be able to be custom-produced on-demand locally. Even if local production by 3D printing is initially more expensive, the elimination of shipping expenses will dramatically change how business is done. 3D printing also allows goods to be tailored to the consumer in a wide range of industries, from medicine to electronics. These advantages, among others, mean that the “factors that have made China the workshop of the world will lose much of their force” in a world in which 3D printing is at the fore. *See, e.g.,* Richard A. D’Aveni, HARVARD BUSINESS REVIEW, 3-D Printing Will Change the World, March 2013. 3D printing gives America the opportunity to revolutionize the way its businesses make and sell products domestically and abroad.

Chilling the speech of actors like Defense Distributed by imposing export controls on them that were never meant to apply domestically will slow innovation in the United States and leave the field to other countries. *See, e.g.,* Michael L. Smith, *The Second Amendment Implications of Regulating 3D Printed Firearms*, 31 SYRACUSE J. OF SCIENCE & TECH. L. REPORTER 60, 95 (2015) (recognizing that “laws that would criminalize the distribution of digital blueprints for firearms” might “unduly constrain technological development”). It is precisely the kind of experimentation and public discussion that Appellants foster that brings the most

unexpected and powerful developments in technology. The digital revolution was forged by individuals working in Silicon Valley garages, not governments. And many innovations that are broadly applicable take root first in the context of arms. *See generally* STUART W. LESLIE, THE COLD WAR AND AMERICAN SCIENCE: THE MILITARY-INDUSTRIAL-ACADEMIC COMPLEX AT MIT AND STANFORD (1993) (explaining how military needs drove innovation in engineering and computing).

Given these powerful reasons to allow technological innovation in 3D printing to grow and flourish, the State Department's insistence that its idiosyncratic interpretation of the AECA should shut down scientific progress is inexplicable. If Appellants' speech is to be regulated—and in reality there is no basis for any such regulation—that work should be done by Congress, not by an administrative agency making it up as it goes along.

CONCLUSION

For the foregoing reasons, the Court should adhere to the text of the AECA and the Constitution, and therefore reverse the district court's order and remand with instructions to enter a preliminary injunction against ITAR's enforcement as a prior restraint.

Respectfully Submitted,

/s/ Raffi Melkonian

Raffi Melkonian
State Bar No. 24090587
WRIGHT & CLOSE, LLP
One Riverway, Suite 2200
Houston, Texas 77056
713-572-4321
713-572-4320 (fax)
melkonian@wrightclose.com

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

This is to certify that on December 17, 2015, a true and correct copy of the foregoing document was filed with the clerk of the court for the United States Court of Appeals for the Fifth Circuit, using the electronic case filing system of the court. The electronic case filing system sent a “Notice of Electronic Filing” to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means. I also certify that a true and correct copy of the foregoing document was served on opposing counsel by mail and e-mail.

/s/ Raffi Melkonian

Raffi Melkonian

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,386 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. 32(a)(6) because this brief has been prepared in proportionally spaced typeface using Microsoft Word 2007 in Times New Roman (Scalable) 14 pt. for text and Times New Roman (Scalable) 12pt for footnotes.

/s/ Raffi Melkonian

Raffi Melkonian

ECF CERTIFICATION

I hereby certify (i) the required privacy redactions have been made pursuant to 5th Cir. R. 25.2.13; (ii) the electronic submission is an exact copy of any paper document submitted pursuant to 5th Cir. R. 25.2.1; (iii) the document has been scanned for viruses and is free of viruses; and (iv) the paper document will be maintained for three years after the mandate or order closing the case issues, pursuant to 5th Cir. R. 25.2.9.

/s/ Raffi Melkonian

Raffi Melkonian

**APPENDIX A
LIST OF AMICUS CURIAE**

Representative Thomas Massie (Kentucky)
Representative Brian Babin (Texas)
Representative K. Mike Conaway (Texas)
Representative Jeff Duncan (South Carolina)
Representative Blake Farenthold (Texas)
Representative John Fleming (Louisiana)
Representative Paul Gosar (Arizona)
Representative Walter Jones (North Carolina)
Representative Mike Kelly (Pennsylvania)
Representative Steve King (Iowa)
Representative Raúl Labrador (Idaho)
Representative Jeff Miller (Florida)
Representative Bill Posey (Florida)
Representative Todd Rokita (Indiana)
Representative Daniel Webster (Florida)

NO. 15-50759

DEFENSE DISTRIBUTED, et al.,
Plaintiffs-Appellants,

v.

UNITED STATES DEPARTMENT OF STATE, et al.,
Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF TEXAS, AUSTIN DIVISION

No. 1:15-cv-00372-RP
The Hon. Robert L. Pitman
United States District Court Judge

***AMICI CURIAE* BRIEF OF THE REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS AND THE THOMAS JEFFERSON CENTER
FOR THE PROTECTION OF FREE EXPRESSION
IN SUPPORT OF APPELLANTS**

J. Joshua Wheeler
THOMAS JEFFERSON CENTER FOR THE
PROTECTION OF FREE EXPRESSION &
THE UNIVERSITY OF VIRGINIA SCHOOL OF LAW
FIRST AMENDMENT CLINIC
400 Worrell Drive
Charlottesville, VA 22911
Telephone: (434) 295-4784
jjw@tjcenter.org

Bruce D. Brown
Counsel of Record
Gregg P. Leslie
Hannah Bloch-Wehba
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
bbrown@rcfp.org

CERTIFICATE OF INTERESTED PERSONS

Defense Distributed, et al. v. U.S. Dep't of State, et al., No. 15-50759

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici* disclose that:

The Reporters Committee for Freedom of the Press is an unincorporated nonprofit association of reporters and editors with no parent corporation and no stock.

The Thomas Jefferson Center for the Protection of Free Expression is a nonprofit organization with no parent corporation and no stock.

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this Court may evaluate possible disqualification or recusal.

Plaintiffs:

Defense Distributed, Second Amendment Foundation, Inc.

Defendants:

U.S. Dep't of State, John F. Kerry, Directorate of Defense Trade Controls, Kenneth B. Handelman, C. Edward Peartree, Sarah J. Heidema, Glenn Smith

Plaintiffs' Counsel:

Alan Gura, Gura & Possessky, PLLC; Matthew A. Goldstein, Matthew A. Goldstein, PLLC; William B. Mateja, William T. "Tommy" Jacks, David Morris, Fish & Richardson P.C.; Josh Blackman

Defendants' Counsel:

Loretta Lynch, Michael S. Raab, Daniel Bentele Hahs Tenny, Eric J. Soskin, Stuart

J. Robinson, Richard L. Durban, Benjamin C. Mizer, Anthony J. Coppolino,
Zachary C. Richter – U.S. Department of Justice

Amici Curiae: Reporters Committee for Freedom of the Press; Thomas Jefferson
Center for the Protection of Free Expression

Counsel for Amici: Bruce D. Brown, Gregg P. Leslie, Hannah Bloch-Wehba –
Reporters Committee for Freedom of the Press; J. Joshua Wheeler – Thomas
Jefferson Center for the Protection of Free Expression

/s/ Bruce D. Brown

Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
bbrown@rcfp.org

TABLE OF CONTENTS

CERTIFICATE OF INTERESTED PERSONS	ii
TABLE OF AUTHORITIES	v
STATEMENT OF INTEREST OF <i>AMICI CURIAE</i>	1
SUMMARY OF ARGUMENT	3
INTRODUCTION	5
ARGUMENT	6
I. The AECA and ITAR are content-based regulations of speech.	6
II. The AECA and ITAR are unconstitutionally overbroad and vague.	11
A. ITAR’s sweeping definitions of “technical data” and “export” reach substantial amounts of protected expression and do not adequately describe the conduct proscribed by the regulations.	12
B. The broad restraints on “export” of “technical data” appear to apply to significant amounts of protected speech.	17
III. The AECA and ITAR provide the DDTC with unlimited, unreviewable discretion to enforce the law.....	22
A. The definitions of “technical data” and “export” in the ITAR do not provide explicit enforcement standards to the DDTC.	24
B. The absence of judicial review exacerbates the ITAR’s overbroad sweep by obscuring the distinction between “permissible” journalism and prohibited speech.....	26
CONCLUSION.....	28
CERTIFICATE OF COMPLIANCE.....	29
CERTIFICATE OF SERVICE	30

TABLE OF AUTHORITIES

CASES

<i>Asgeirsson v. Abbott</i> , 696 F.3d 454 (5th Cir. 2012)	8
<i>Baggett v. Bullitt</i> , 377 U.S. 360 (1964)	23
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001)	18
<i>City of Houston v. Hill</i> , 482 U.S. 451 (1987)	12, 21
<i>Connally v. General Construction Co.</i> , 269 U.S. 385 (1926)	13
<i>Consolidated Edison Co. of N. Y. v. Public Serv. Comm'n of N. Y.</i> , 447 U. S. 530 (1980)	9
<i>Cramp v. Board of Public Instruction</i> , 368 U.S. 278 (1961)	23
<i>Dombrowski v. Pfister</i> , 380 U.S. 479 (1965)	21
<i>Erzonznik v. City of Jacksonville</i> , 422 U.S. 205 (1975)	12
<i>Freedman v. Maryland</i> , 380 U.S. 51 (1965)	10
<i>Grayned v. City of Rockford</i> , 408 U.S. 104 (1972).	13, 16
<i>Hynes v. Mayor & Council of Oradell</i> , 425 U.S. 610 (1976)	13
<i>Kagan v. City of New Orleans, La.</i> , 753 F.3d 560 (5th Cir. 2014)	8
<i>NAACP v. Button</i> , 371 U.S. 415 (1963)	12, 17, 27
<i>National Endowment of the Arts v. Findley</i> , 524 U.S. 569 (1998)	23
<i>Reed v. Town of Gilbert, Ariz.</i> , 135 S.Ct. 2218 (2015)	3, 10
<i>Smith v. Daily Mail Pub. Co.</i> , 443 U.S. 97 (1979)	18, 22

<i>Sorrell v. IMS Health Inc.</i> ,	
131 S. Ct. 2653 (2011)	8
<i>Thomas v. Chicago Park Dist.</i> ,	
534 U.S. 316 (2002)	10
<i>United States ex rel. McGrath v. Microsemi Corp.</i> ,	
No. CV-13-00854-PHX-DJH, 2015 WL 6121568 (D. Ariz. Sept. 30, 2015)	26
<i>United States v. Chi Mak</i> ,	
683 F.3d 1126 (9th Cir. 2012)	9, 17, 27
<i>United States v. Hsu</i> ,	
364 F.3d 192 (4th Cir. 2004)	17
<i>United States v. Huynh</i> ,	
246 F.3d 734 (5th Cir. 2001)	14
<i>United States v. Roth</i> ,	
628 F.3d 827 (6th Cir. 2011)	26
<i>United States v. Stevens</i> ,	
559 U.S. 460 (2010)	12
<i>United States v. Zhen Zhou Wu</i> ,	
711 F.3d 1 (1st Cir. 2013)	15, 16
<i>Village of Hoffman Estates et al. v. The Flipside, Hoffman Estates, Inc.</i> ,	
455 U.S. 489 (1989)	14, 23
<i>Washington State Grange v. Washington State Republican Party</i> ,	
552 U.S. 442 (2008)	22
<i>Williams v. Rhodes</i> ,	
393 U.S. 23 (1968)	27

STATUTES

Arms Export Control Act (“AECA”), Pub. L. 94-329, tit. II, 90 Stat. 729 (1976), 22 U.S.C. § 2751	passim
---	--------

OTHER AUTHORITIES

Bryan Schatz, <i>How US Cluster Bombs Banned by Most Countries Ended Up in Yemen</i> , Mother Jones (Jun. 9, 2015)	24
Declan McCullagh, <i>DHS Built Domestic Surveillance Tech into Predator Drones</i> , CNET (Mar. 2, 2013)	17, 18
Exec. Order No. 11,958, 42 Fed. Reg. 4311 (Jan. 18, 1977)	5
Mukesh G. Harisinghani et al., <i>Noninvasive Detection of Clinically Occult Lymph-Node Metastases in Prostate Cancer</i> , 348 NEW ENG. J. MED. 2491 (2003)	20
Proposed Charging Letter, Analytical Methods, Inc. (Dec. 19, 2008)	10

R. Scott Kemp, <i>Is This Where North Korea Makes Its Centrifuges?</i> Arms Control Wonk (June 24, 2013)	18
Richard G. Stevens et al., <i>Body Iron Stores and the Risk of Cancer</i> , 319 NEW ENG. J. MED. 1047 (1988).....	20

REGULATIONS

International Traffic in Arms Regulations, 22 C.F.R. pt. 120	passim
International Traffic in Arms, 80 Fed. Reg. 31,525 (proposed June 3, 2015) (to be codified at 22 C.F.R. pt. 120)	13, 15, 17, 21
United States Munitions List (“USML”), 22 C.F.R. § 121.1.....	passim

STATEMENT OF INTEREST OF *AMICI CURIAE*¹

The Reporters Committee for Freedom of the Press and the Thomas Jefferson Center for the Protection of Free Expression submit this *amici curiae* brief in support of Petitioners-Appellants.

The Reporters Committee for Freedom of the Press is an unincorporated nonprofit association of reporters and editors that works to safeguard the First Amendment's guarantee of a free and unfettered press, and the public's right to be informed, through the news media, about the government. The Reporters Committee has provided guidance and research in First Amendment and freedom of information litigation since 1970.

The Thomas Jefferson Center for the Protection of Free Expression is a nonprofit, nonpartisan organization located in Charlottesville, Virginia. Founded in 1990, the Center has as its sole mission the protection of free speech and press. The Center has pursued that mission in various forms, including the filing of *amici curiae* briefs in this and other federal courts, and in state courts around the country.

¹ Pursuant to Rule 29(c)(5) of the Federal Rules of Appellate Procedure, *amici* state that no party's counsel authored this brief in whole or in part, and no party, party's counsel, or any other person, other than the *amici curiae*, their members, or their counsel, contributed money that was intended to fund preparing or submitting the brief. Pursuant to Rule 29(c)(4), all parties have consented to the filing of this brief.

This case is of particular importance to *amici* because the district court below erred in holding that the Arms Export Control Act (“AECA”), Pub. L. 94-329, tit. II, 90 Stat. 729 (1976), 22 U.S.C. § 2751 et seq., and its implementing regulations, the International Traffic in Arms Regulations (“ITAR”), 22 C.F.R. §§ 120–130, do not violate the First Amendment.

SUMMARY OF ARGUMENT

This case arises out of Plaintiffs’ challenge to the constitutionality of the International Traffic in Arms Regulations (“ITAR”), 22 C.F.R. §§ 120–130, which purport to require Plaintiffs to obtain a license before publishing certain information allegedly related to national defense on the Internet. The Arms Export Control Act (“AECA”), Pub. L. 94-329, tit. II, 90 Stat. 729 (1976), 22 U.S.C. § 2751 et seq., regulates the trade of “defense articles and defense services.” *Id.* § 2778(a)(1). The Act’s implementing regulations, the ITAR, include the United States Munitions List (“USML”), 22 C.F.R. § 121.1, the list of all defense articles, services, and related “technical data” whose “export” requires a license. *See id.* § 121.1(b)(2) (“Most U.S. Munitions List categories contain an entry on technical data . . .”). The ITAR requires that a person who wishes to export “technical data” first “obtain the approval of the Directorate of Defense Trade Controls,” the component of the Department of State that administers the regulations. 22 C.F.R. § 123. Violation of the AECA is a criminal offense punishable by a fine up to \$1 million, twenty years in prison, or both. 22 U.S.C. § 2778(c).

At issue in this case is the constitutionality of the licensing requirement for exporting “technical data.” The decision below erroneously “conflates two distinct but related limitations that the First Amendment places on government regulation of speech,” *Reed v. Town of Gilbert, Ariz.*, 135 S.Ct. 2218, 2230 (2015),

concluding that because the ITAR’s ban on unlicensed export of “technical data” is a viewpoint-neutral speech restriction, it is content-neutral as well. As the Supreme Court explained in *Town of Gilbert*, however, restrictions may be impermissibly content-based despite being viewpoint-neutral. The decision below failed to account for this possibility and thus failed to impose the appropriate standard of scrutiny in analyzing the restrictions at issue here.

Second, the ITAR’s restrictions on the “export” of “technical data” are both overbroad and vague. The AECA and ITAR are overbroad because they burden significant amounts of speech protected by the First Amendment, including reporting and online journalism. The ITAR’s definitions of the terms “export” and “technical data” reach far beyond the ordinary meaning of those words, and unquestionably tread on lawful speech and publication acts. The AECA and ITAR also allow the government practically unfettered discretion as to the scope of proscribed activity, and exempt government decision-making from judicial review. Even on its own terms, the ITAR presents practically unlimited definitions of “technical data” and “export” that are incomprehensible to reasonable citizens. As a result, the ITAR threatens to punish not only legitimate trade violations but substantial amounts of protected speech as well.

INTRODUCTION

At issue in this case are a broad and sweeping set of regulations that purport to criminalize the dissemination of certain “technical data” without a license. Although the statute and regulations at issue in this case are meant to curb the unauthorized import and export of arms and other defense articles, they also restrict the dissemination of “related technical data” without a license. This restraint is an unlawful content-based speech restriction. *See infra* pp. 4–10.

Even more troubling, however, is the government’s assertion of broad and sweeping authority to punish protected speech that happens to include “technical data.” The overbroad and vague definitions of “export” and “technical data” appear to cover lawful publication of journalism on important matters of public interest, including reporting on the United States’ drone programs, *see infra* p. 17, North Korean nuclear enrichment, *see infra* pp. 18–19, or even medical breakthroughs using iron powder, *see infra* p. 19. Although the Defendants have not sought to apply these regulations to journalists or reporters, the government appears to possess unfettered discretion under the regulations to do so. The absence of judicial review raises further concerns that an already overbroad regulatory regime may be applied to limit First Amendment-protected speech in an unlawful manner. *Amicus* writes to emphasize that the regulations at issue here deter protected speech on important matters of public concern.

ARGUMENT

I. The AECA and ITAR are content-based regulations of speech.

The Arms Export Control Act (“AECA”) controls the “import and the export of defense articles and defense services.” 22 U.S.C. § 2778(a)(1). Items designated as “defense articles and defense services” comprise the United States Munitions List (the “Munitions List”), a part of the International Traffic in Arms Regulations (“ITAR”), the implementing regulations for the AECA. The President has delegated his authority to designate “defense articles and services” to the State Department. Exec. Order No. 11,958, 42 Fed. Reg. 4311 (Jan. 18, 1977).

The Munitions List is a long list of “articles, services and related technical data,” the export of which is proscribed without a license. 22 C.F.R. § 121.1. “Technical data” is information “required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles,” specifically including “blueprints, drawings, photographs, plans, instructions or documentation.” 22 C.F.R. § 120.10; *see also id.* at § 121.1(I)(i) (defining as “technical data” any data “directly related to the defense articles described in paragraphs (a) through (h) of this category,” including data related to rifle scopes and “cylinders”); *id.* § 121.1(II)(k) (using a similar definition, which in Category II includes data concerning tooling and “diagnostic instrumentation”).

It is undisputed that “technical data” can amount to protected speech. As a result, the court below was correct in finding that the ITAR “unquestionably regulates speech concerning a specific topic.” ROA.691. Nonetheless, the court went on, “The ITAR does not regulate disclosure of technical data based on the *message* it is communicating.” *Id.* As a result, the court concluded that the ITAR is not content based because the regulations are “intended to satisfy a number of foreign policy and national defense goals.” *Id.*

The court’s conclusion that a regulation is content neutral so long as it is not based on message has no foundation. “A speech regulation targeted at specific subject matter is content based even if it does not discriminate among viewpoints within that subject matter.” *Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2230 (2015). *Town of Gilbert* recognizes that laws that “single[] out specific subject matter for differential treatment,” as ITAR does, are facially content based and subject to strict scrutiny. *Id.*

ITAR creates numerous distinctions on the basis of the content of protected speech. The regulations distinguish “technical” data from data that is presumably “nontechnical,” and proscribe the unlicensed publication only of technical data “related” to designated defense articles. 22 C.F.R. § 121.1 (“Most U.S. Munitions List categories contain an entry on technical data . . . and defense services . . . related to the defense articles described in that U.S. Munitions List category.”). As

in *Town of Gilbert*, the regulation at issue here singles out and distinguishes types of speech that are permissible from those that are not. 22 C.F.R. § 120.10 (distinguishing “technical data” from information “commonly taught” in institutions of learning, “information in the public domain,” “basic marketing information,” or “general system descriptions of defense articles”) (*cf. Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2663 (2011) (statutory exemption permitting “educational communications” but not marketing was facially content-based)).

ITAR is also fundamentally unlike content neutral regulatory schemes that the Fifth Circuit has previously upheld. Last year, this Court upheld a provision of the New Orleans Code requiring a license for a person to charge for tours of City points of interest and historic sites, concluding that the licensing requirement “has no effect whatsoever on the content of what tour guides say.” *Kagan v. City of New Orleans, La.*, 753 F.3d 560, 562 (5th Cir. 2014) *cert. denied*, 135 S. Ct. 1403 (2015). In contrast, the regulations at issue here are explicitly designed to affect the content of speech that includes technical data.

Likewise, in 2012, this Court upheld provisions of the Texas Open Meetings Act that criminalized discussion of public matters by a quorum of public officials outside of an open meeting, finding that the statute was content neutral because its “purpose is to control the secondary effects of closed meetings.” *Asgeirsson v. Abbott*, 696 F.3d 454, 461 (5th Cir. 2012). This Court distinguished the Act,

which “is applicable only to private forums and is designed to *encourage* public discussion,” from content based regulations that discourage protected speech in public forums. *Id.* (citing *Burson v. Freeman*, 504 U.S. 191 (1992)). In contrast, the ITAR unquestionably applies to restrict speech on specific topics in public forums, and operates to deter, not encourage, expression. *See* ROA.689 (acknowledging that the World Wide Web is a public forum). As a result, although the ITAR is intended to address the export of defense articles and services, its restrictions on “technical data” unquestionably have a substantial effect on expression and speech as well.

Likewise, this Court should reverse the District Court’s conclusion that the ITAR is content neutral because it “does not regulate disclosure of technical data based on the *message* it is communicating.” ROA.691. The District Court’s approach flouts the constitutional rule that “[t]he First Amendment’s hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic.” *Consolidated Edison Co. of N.Y. v. Public Serv. Comm’n of N.Y.*, 447 U. S. 530, 537 (1980). Similarly, the Ninth Circuit’s conclusion that the ITAR is content neutral because it “defines the technical data based on its *function* and not its viewpoint” contravenes the express holding in *Town of Gilbert. United States v. Chi Mak*, 683 F.3d 1126, 1135 (9th Cir. 2012). Nor can the regulations be saved by their

purported overall purpose: a government's purpose is not relevant to the interpretation of a facially content-based regulation. *Town of Gilbert*, 135 S.Ct. at 2228 (“That is why we have repeatedly considered whether a law is content neutral on its face *before* turning to the law's justification or purpose.”).

Finally, because the ITAR is a content-based regulation that requires licensing, it is a classic prior restraint and requires adequate safeguards under *Freedman v. Maryland*, 380 U.S. 51 (1965). Content-based licensing requirements such as the one at issue here must satisfy demanding requirements:

- (1) any restraint prior to judicial review can be imposed only for a specified brief period during which the status quo must be maintained;
- (2) expeditious judicial review of that decision must be available; and
- (3) the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof once in court.”

Thomas v. Chicago Park Dist., 534 U.S. 316, 321 (2002) (citing *Freedman v. Maryland*, 380 U.S. at 58–60).

The ITAR cannot satisfy these requirements because it explicitly limits the availability of judicial review. Under the AECA and ITAR, the Directorate of Defense Trade Controls (“DDTC”), a component of the State Department, has discretion to treat nearly any piece of research as technical data, and these decisions “shall not be subject to judicial review.” 22 U.S.C. § 2778(h).

This unreviewable use of discretion allows the DDTC to treat many types of research as technical data subject to export controls. For example, the DDTC has brought enforcement actions against companies on the basis that physics modeling software is technical data, since it could possibly be used for weapons development. *See, e.g.*, Proposed Charging Letter, Analytical Methods, Inc. (Dec. 19, 2008), *available at* <https://goo.gl/H7YpTs>. Further, the DDTC considers technical data to include information about ammunition for any firearm up to and including .50 caliber—thus, ITAR bans the unlicensed dissemination even of information on bullets for a standard home-defense handgun. *See* 22 C.F.R. § 121.1(III)(e). ITAR also bans the publication of “technical data” about face paints, helmets, goggles, and visors. *See id.* § 121.1(X)(e). In short, the USML includes not only seemingly everything that could to any degree be connected with the military, but also any “technical data” about those same things.

II. The AECA and ITAR are unconstitutionally overbroad and vague.

The AECA and ITAR are overbroad because they levy criminal and civil penalties upon the unlicensed “export” of “technical data” without adequately defining those terms to ensure that legitimate speech goes unpunished.

“The objectionable quality of vagueness and overbreadth does not depend upon the absence of fair notice to a criminally accused or upon unchanneled

delegation of legislative powers, but upon a danger of tolerating, in the area of First Amendment freedoms, the existence of a penal statute susceptible of sweeping and improper application.” *NAACP v. Button*, 371 U.S. 415, 432–33 (1963). The AECA and ITAR present precisely this danger.

- A. ITAR’s sweeping definitions of “technical data” and “export” reach substantial amounts of protected expression and do not adequately describe the conduct proscribed by the regulations.

The AECA’s criminalization of the unlicensed “export” of “technical data” is unconstitutionally overbroad because the key terms “export” and “technical data” reach significant amounts of protected speech.

To satisfy an overbreadth challenge, a plaintiff must show that the challenged statute is not subject to a narrowing construction and has a real and substantial deterrent effect on legitimate expression. *Erzonznik v. City of Jacksonville*, 422 U.S. 205, 216 (1975); *see also United States v. Stevens*, 559 U.S. 460, 474 (2010) (stating that the first step of an overbreadth challenge is to determine the scope of the law at issue). Criminal statutes, such as those at issue here, “that make unlawful a substantial amount of constitutionally protected conduct may be held facially invalid even if they also have a legitimate application.” *City of Houston v. Hill*, 482 U.S. 451, 459 (1987).

A law is unconstitutionally vague if it does not “give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may

act accordingly.” *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). The Supreme Court has held that “the general test of vagueness applies with particular force in review of laws dealing with speech.” *Hynes v. Mayor & Council of Oradell*, 425 U.S. 610, 620 (1976). In *Hynes*, the Court reasoned that the importance of the “free dissemination of ideas” was such that a heightened standard for clarity was appropriate. *Id.*; *see also Connally v. General Construction Co.*, 269 U.S. 385, 391 (1926) (noting that a statute is vague when “men of common intelligence must necessarily guess at its meaning and differ as to its applications”).

The State Department, which implements ITAR, has interpreted the term “export” broadly, to include publication on the Internet: “providing technical data on a publicly accessible network, such as the Internet, is an export because of its inherent accessibility to foreign powers.” Defs.’ Opp. to Pl.’s Mot. for Preliminary Inj. at 3 n.2, 1:15-cv-00372-RP (June 10, 2015), ECF No. 132. As an initial matter, it is evident that the term “export” touches on First Amendment freedoms. DDTC has defined “export” to include “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad.” 22 C.F.R. § 120.17(a)(4). As applied to goods such as defense articles, it is unambiguous that the word “export” “does not require proof that the goods actually arrived in the foreign country.” *See United States v. Huynh*, 246

F.3d 734, 741 (5th Cir. 2001) (“Exportation occurs when the goods are shipped to another country with the intent that they will join the commerce of that country, not when they arrive in that country.”). While the District Court concluded that “persons of ordinary intelligence are clearly put on notice by the language of the regulations” that online publication “would fall within the definition of export,” ROA.702, that definition strays considerably from the ordinary meaning of the word.

As a result, there is no question that the State Department has not offered a narrowing construction of “export” that would save the statute. *See Village of Hoffman Estates et al. v. The Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 494 n.5 (1989) (“In evaluating a facial challenge to a state law, a federal court must, of course, consider any limiting construction that a state court or enforcement agency has proffered.”). Indeed, under proposed regulations, ITAR’s definition of “export” would be expanded to expressly include “[m]aking technical data available via a publicly available network (*e.g.*, the Internet).” International Traffic in Arms, 80 Fed. Reg. 31,525, 31,535 (proposed June 3, 2015) (to be codified at 22 C.F.R. § 120.17(a)(7)). According to the Department, this proposed definition “makes more explicit the existing control in (a)(4).” *Id.* at 31,529. In other words, the State Department already reads “export” expansively, and its proposed rules are intended merely to codify this.

The definition of “technical data” is similarly overbroad. The DDTC controls the export of technical data largely through its maintenance of the USML, which describes what technology is subject to the AECA. Though many of the entries in the USML refer to actual military hardware, the Munitions List consistently includes technical data “related to” those articles. *See, e.g.*, 22 C.F.R. § 121.1(I)(i), (II)(k). In addition to specifically enumerating various types of technical data, the USML also broadly notes that technical data related to broad categories of “defense articles” considered “significant military equipment”—including explosives, propellants, and aircraft—are defense items themselves. *See id.* § 121.1(b). Further, the USML also includes a catch-all provision allowing the DDTC to include any article or technical data not otherwise listed which has “substantial military applicability.” *Id.* § 121.1(XXI). Still further, the USML is not even an exhaustive list of export-controlled items but rather a “series of categories describing the *kinds* of items that qualify as ‘defense articles’ requiring export licenses.” *United States v. Zhen Zhou Wu*, 711 F.3d 1, 12 (1st Cir. 2013) *cert. denied sub nom. Yufeng Wei v. United States*, 134 S. Ct. 365 (2013) (emphasis added).

Indeed, the very terms designed to limit the scope of the ITAR’s restraint on publication of “technical data”—“required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or

modification of defense articles”—actually create an expansive definition that “sweeps within its prohibitions what may not be punished under the First and Fourteenth Amendments.” *City of Rockford*, 408 U.S. at 113, 115 (upholding an antinoise ordinance because it “contains no broad invitation to subjective or discriminatory enforcement”); *see also Cox v. Louisiana*, 379 U.S. 536, 5512 (1965) (striking down a Louisiana criminalizing “breach of the peace”. In its proposed rule, the Department of State notes, “‘Required’ is used in the definition of ‘technical data’ and has, to this point, been an undefined term in the ITAR.” 80 Fed. Reg. at 31,527. The proposed new definition of “required” in the NPRM remains quite vague, and “explicitly includes information for meeting not only controlled performance levels, but also characteristics and functions.” *Id.* As DDTC explains in relation to the example of controlled “bomber” aircraft,” “The characteristic of the aircraft that is controlled is that it is a bomber, and therefore, any ‘technical data’ peculiar to making an aircraft a bomber is ‘required.’” *Id.* This explanation hardly clarifies or limits the scope of the definition.

Moreover, while the District Court was correct that “at least two circuits have rejected due process challenges to the AECA and ITAR, and upheld criminal convictions for its violation,” both of those circuits considered the vagueness of the statute as applied to export of defense articles, not technical data comprising speech. *See Zhen Zhou Wu*, 711 F.3d at 12 (denying vagueness challenge to ITAR

as applied to defendants convicted of unlicensed export of phase shifters); *United States v. Hsu*, 364 F.3d 192, 198 (4th Cir. 2004) (denying vagueness challenge as applied to defendants convicted of conspiracy to violate ITAR by exporting encryption devices); *but see also Chi Mak*, 683 F.3d at 1135–36 (reviewing vagueness claim related to “technical data” provision for plain error). In contrast, the “technical data” provision clearly implicates First Amendment rights, and courts cannot assume that the government will exercise its prosecutorial discretion with a careful eye toward not violating the First Amendment. *NAACP v. Button*, 371 U.S. at 438 (“Precision of regulation must be the touchstone in an area so closely touching our most precious freedoms.”).

On top of these definitions, ITAR offers exceptions for general scientific principles “commonly taught in schools, colleges, and universities or information in the public domain.” 22 C.F.R. § 120.10(b). The “public domain exception” covers research from accredited universities that is ordinarily published and shared in the field. *Id.*; *id.* at § 120.11 (defining “public domain”). In proposed amendments to ITAR, the Department of State has recognized that the exception is “unnecessarily limiting in scope and insufficiently flexible with respect to the continually evolving array of media, whether physical or electronic, through which information may be disseminated.” 80 Fed. Reg. 31527.

- B. The broad restraints on “export” of “technical data” appear to apply to significant amounts of protected speech.

Under the ITAR, posting “technical data” to a domestic website, or publishing the same information in a domestic publication, becomes an “export” under the AECA whenever a foreign citizen reads that information. This definition raises serious First Amendment concerns, as it suggests that publication of facts lawfully obtained may be a violation of the ITAR. *See Bartnicki v. Vopper*, 532 U.S. 514, 528 (2001) (“[S]tate action to punish the publication of truthful information seldom can satisfy constitutional standards.”), *citing Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 102 (1979).

For example, when an online news outlet publishes “technical data” which it has “lawfully obtained,” but which is not in the public domain, the capacious definition of “export” suggests that publication is a violation of export controls. In 2013 technology reporters at CNET published an article relating to the Predator drones used by the U.S. Military. Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET (Mar. 2, 2013), <http://www.cnet.com/news/dhs-built-domestic-surveillance-tech-into-predator-drones/>. Although the Department of Homeland Security had offered a redacted document listing performance requirements for unmanned surveillance drones in response to a Freedom of Information Act request, the article included a link to an “unredacted copy” of that same document that CNET had obtained lawfully. *Id.* If the unredacted copy included “technical data,” CNET’s publication would appear

to constitute an ITAR violation. At the same time, the technical specifications of the drone were central to the article, which considered whether the DHS was using or developing technology that would enable domestic surveillance. *Id.* Likewise, search engines, research databases, library catalogs, and other online resources that include links to “technical data” may “export” that information by making it available to users abroad.

Similarly, in 2013, the Arms Control Wonk blog published a post by R. Scott Kemp, Norman C. Rasmussen Assistant Professor of Nuclear Science and Engineering at the Massachusetts Institute of Technology, republishing photographs of Kim Jong-un’s trip to a factory that may be used to manufacture centrifuges. R. Scott Kemp, *Is This Where North Korea Makes Its Centrifuges?* Arms Control Wonk (June 24, 2013), *available at* www.armscontrolwonk.com/archive/206637/is-this-where-north-korea-makes-its-centrifuges/. The post included photographs and discussion of flow-forming machines that are “the only way to manufacture the thin-walled P-2 centrifuge rotor on which the North Korean enrichment program is thought to be built.” *Id.* The post describes the flow-forming machine as “part of an assembly-line fabrication process for making thin-walled components” for centrifuges. *Id.*

The plain text of the ITAR indicates that the information included in Professor Kemp’s blog post, although general and speculative, may be “technical

data.” It is clear that the photographs in the post include information “required” for the design, operation, or manufacture of a centrifuge, which is “specifically designed or modified for use in the design, development, or fabrication of nuclear weapons or nuclear explosive devices.” 22 C.F.R. § 120.10 (defining “technical data” as information “required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles,” specifically including “blueprints, drawings, photographs, plans, instructions or documentation”); *id.* § 121.1(XVI) (“Nuclear Weapons, Design and Testing Related Items”). In this case, photographs of machines required for the manufacture of centrifuges, although obtained from a publicly available source, may not be within ITAR’s “public domain exception” because they were republished online from North Korean state media, not available “through sales at newsstands and bookstores,” through subscriptions, or through “second class mailing privileges.” *Id.* § 120.11.

The State Department’s construction of “technical data” discourages the press from discussing matters of great public importance, even if unrelated to defense. For example, iron may be used to detect certain forms of cancer, whether by utilizing it or by measuring it in the body. *See, e.g.,* Mukesh G. Harisinghani et al., *Noninvasive Detection of Clinically Occult Lymph-Node Metastases in Prostate Cancer*, 348 NEW ENG. J. MED. 2491 (2003); Richard G. Stevens et al.,

Body Iron Stores and the Risk of Cancer, 319 NEW ENG. J. MED. 1047 (1988). At the same time, the USML includes “[i]ron powder . . . with a particle size of 3 micrometers or less produced by reduction of iron oxide with hydrogen.” 22 C.F.R. § 121.1(V)(c)(4)(i)(B). A journalist covering innovations in healthcare who wants to report on unpublished research concerning iron powder’s utility in cancer treatment may be unable to do so under the ITAR. And courts may not assume that, should the reporter be prosecuted for this violation, her constitutional rights would be properly vindicated in the course of her defense. *See Dombrowski v. Pfister*, 380 U.S. 479, 486 (1965) (“When the statutes also have an overbroad sweep . . . the hazard of loss or substantial impairment of [First Amendment] rights may be critical. . . . The assumption that defense of a criminal prosecution will generally assure ample vindication of constitutional rights is unfounded in such cases.”).

Indeed, the proposed changes to ITAR make clear that “the *further* dissemination of ‘technical data’ or software that was made available to the public without authorization is a violation of the ITAR if, and only if, it is done with knowledge that the ‘technical data’ or software was made publicly available without an authorization.” 80 Fed. Reg. at 31,528 (emphasis added). This interpretation of ITAR touches on significant amounts of protected expression. *Hill*, 482 U.S. at 459. A regulation that criminalizes news coverage of facts that

are lawfully obtained but that comprise “technical data” runs counter to the First Amendment. *Cf. Daily Mail Pub. Co.*, 443 U.S. at 103 (“[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.”).

That the plain language of ITAR’s prohibition on unlicensed export of “technical data” would suppress speech like that in Professor Kemp’s blog post illustrates the overbreadth problem that inheres in the ITAR. The sweeping definitions of the terms “export” and “technical data” are further amplified when the two are read together, creating a real and substantial deterrent effect on speech. The substantiality of a deterrent effect is judged by the number of unconstitutional applications in relation to the statute’s “plainly legitimate sweep.” *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 449 n.6 (2008); *see also United States v. Williams*, 553 U.S. 285, 292 (2008). This deterrence affects not only researchers and members of the defense community, but also the public more broadly, especially the press.

III. The AECA and ITAR provide the DDTC with unlimited, unreviewable discretion to enforce the law.

The district court also erred in determining that the ITAR and AECA are not impermissibly vague. Indeed, under this regulatory scheme, no reasonable citizen

could predict whether a particular piece of information regarding the design, operation, repair, or testing of “defense articles” is “required” for that task, and thus whether it is covered by the AECA and ITAR.

A statute may be vague if it gives too much discretion to the party that enforces it. In *Cramp v. Board of Public Instruction*, the Supreme Court invalidated a Florida statute that required state employees to swear an oath that they had never supported the Communist Party. 368 U.S. 278, 279 (1961). The Court explained that the oath was vague partly because it lacked any “terms susceptible of objective measurement.” *Id.* at 286. This deficiency provoked the Court to note that the oath allowed prosecution for “guiltless knowing behavior” at the decision of those “always ready to affix a Communist label upon those whose ideas they violently oppose.” *Id.* at 287. Because the statute could be used to prosecute guiltless behavior at the prosecutor’s whim, it was unconstitutionally vague. *Id.*; see also *National Endowment of the Arts v. Findley*, 524 U.S. 569, 588 (1998) (finding that the First Amendment protects people from “arbitrary and discriminatory enforcement of vague standards”); *Baggett v. Bullitt*, 377 U.S. 360 (1964) (invalidating another oath statute on similar grounds). The vagueness standard applies with particular force to statutes that affect First Amendment rights. See *Village of Hoffman Estates*, 455 U.S. at 498 (1982).

The AECA and ITAR are vague under both formulations of the standard. As discussed above, the statutory terms “technical data” and “export” do not adequately inform a citizen regarding what conduct they cover. Because the DDTC has effectively unlimited discretion in applying these terms to specific conduct, the AECA and ITAR are unconstitutionally vague.

A. The definitions of “technical data” and “export” in the ITAR do not provide explicit enforcement standards to the DDTC.

The AECA and ITAR confer unbridled discretion on the DDTC to enforce them. Specifically, the DDTC has complete control over the USML. “The designation by the President (or by an official to whom the President’s functions under subsection (a) have been duly delegated), in regulations issued under this section, of items as defense articles or defense services for purposes of this section *shall not be subject to judicial review.*” 22 U.S.C. § 2778(h) (emphasis added).

Nonetheless, the DDTC’s unilateral and unreviewable discretion with regard to the contents of the USML, and thus with regard to the content of the term “technical data,” means the AECA lacks explicit standards to govern the proscribed conduct.

The AECA and ITAR are also vague with respect to the term “export” because they give the DDTC unlimited discretion to decide what activities are covered. Although the definition of “export” facially covers any disclosure or transfer of export-controlled information to a foreign person, in the instant case the

DDTC has interpreted this to include mere publication to the Internet. If such publication is a fair interpretation of the AECA and ITAR, then almost any Internet posting is subject to government censorship. Further, because the definition turns on whether the information is received by a “foreign person,” even a purely domestic, traditional publication might qualify as an “export” if it is read by a foreign citizen on United States soil. Given this construction of the term, the DDTC has virtually unlimited discretion to selectively pursue prosecutions under the AECA and ITAR for unlawful “export” of “technical data.”

As long as the DDTC may treat any publication that could be read by a foreign citizen as an “export” under the statute, that agency has broad license to quash publications of all sorts. For example, whether a journalist or other Internet user may post an article to a website discussing the moral, ethical, and legal implications of certain cluster bombs that purport to be 99 percent effective is unclear. *See, e.g.,* Bryan Schatz, *How US Cluster Bombs Banned by Most Countries Ended Up in Yemen*, Mother Jones (Jun. 9, 2015), <http://bit.ly/1QIYwS8> (describing the Textron CBU-105 Sensor Fuzed Weapon). Under the AECA, the permissibility of publication would turn on whether the article is available to a foreign national.

Nor does the Government’s suggestion that a publisher’s liability can be limited by taking steps to locate users based on Internet Protocol addresses resolve

this issue. Defs.’ Opp. to Pl.’s Mot. for Preliminary Inj. at 3 n.2, 1:15-cv-00372-RP (June 10, 2015), ECF No. 132. Even if a journalist manages to ensure that her publication is not available overseas, access by a foreign national on domestic soil may still qualify as a violation of the statute. Although the DDTC has generally not prosecuted such cases, nothing in the AECA or ITAR prevents it from doing so. *Cf. United States v. Roth*, 628 F.3d 827, 830–32 (6th Cir. 2011) (affirming professor’s conviction of ITAR violations, partly on grounds that he allowed graduate research assistants who were foreign nationals access to technical data); *see also United States ex rel. McGrath v. Microsemi Corp.*, No. CV-13-00854-PHX-DJH, 2015 WL 6121568, at *10–11, *40–43 (D. Ariz. Sept. 30, 2015) (treating access to ITAR-controlled technical data by foreign employees as a possible violation of ITAR, though the court ultimately held there was no violation on the facts of the case). Consequently, journalists writing about technical aspects of defense issues—or, given the instant case, even gun control—risk receiving a cease and desist letter or criminal charges at the DDTC’s sole discretion.

B. The absence of judicial review exacerbates the ITAR’s overbroad sweep by obscuring the distinction between “permissible” journalism and prohibited speech.

Taken together, these broad definitions unquestionably reach protected speech, but the AECA also provides that executive branch decisions to add or remove an item from the USML “shall not be subject to judicial review.” 22

U.S.C. § 2778(h). The Ninth Circuit has held that this portion of the statute provides the DDTC with the ability to decide whether documents are “technical data” subject to export controls. *United States v. Chi Mak*, 683 F.3d 1126, 1132 (9th Cir. 2012) (holding that the AECA “expressly prohibits judicial review” of such decisions).

Partly as a result of the absence of judicial review, it is difficult to establish bright lines between prohibited disclosures of “technical data,” on the one hand, and permissible journalistic coverage of scientific and technological issues, on the other. *See Button*, 371 U.S. at 438 (highlighting the importance of clarity in laws affecting the First Amendment). The absence of judicial review only exacerbates the First Amendment problems, because the question of whether an online publication constitutes protected speech or “technical data” is not one that may be left to the executive branch to decide. Infringements of First Amendment rights are quintessentially judicial questions. *See Williams v. Rhodes*, 393 U.S. 23, 40 (1968) (Douglas, J., concurring) (“First Amendment rights . . . have a well-established claim to inclusion in justiciable, as distinguished from ‘political,’ questions . . .”). The statute’s provision regarding the unreviewable authority to designate “defense articles” therefore should not extend to the definition of “technical data,” which includes a significant amount of protected speech.

This confluence of the DDTC's unilateral and unreviewable discretion to establish sweeping export prohibitions, on one hand, and overly narrow exceptions to the AECA, on the other, means that the DDTC has an effective veto over online publication of any information it considers to be in some way defense related. This complete control and wide discretion present a real, substantial deterrent to those seeking to discuss or report on matters of technology.

CONCLUSION

For the foregoing reasons, *amici curiae* respectfully urge this Court to reverse.

/s/ Bruce D. Brown
Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-face and volume limitations set forth in Fed. R. of App. P. 32(a)(7)(B) as follows: The type face is fourteen-point Times New Roman font, and the word count is 6,152, excluding the portions of the brief exempted by Rule 32(a)(7)(B)(iii).

/s/ Bruce D. Brown

Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005

CERTIFICATE OF SERVICE

I hereby certify that on December 17, 2015, an electronic copy of the foregoing brief was filed with the Clerk of Court for the United States Court of Appeals for the Fifth Circuit using the Court's CM/ECF system and was served electronically by the Notice of Docket Activity upon all parties in the case. I certify that all participants in the case are CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Bruce D. Brown

Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT**

United States Court of Appeals
Fifth Circuit

FILED

September 20, 2016

Lyle W. Cayce
Clerk

No. 15-50759

DEFENSE DISTRIBUTED; SECOND AMENDMENT FOUNDATION,
INCORPORATED,

Plaintiffs - Appellants

v.

UNITED STATES DEPARTMENT OF STATE; JOHN F. KERRY, In His
Official Capacity as the Secretary of the Department of State;
DIRECTORATE OF DEFENSE TRADE CONTROLS, Department of State
Bureau of Political Military Affairs; KENNETH B. HANDELMAN,
Individually and in His Official Capacity as the Deputy Assistant Secretary
of State for Defense Trade Controls in the Bureau of Political-Military
Affairs; C. EDWARD PEARTREE, Individually and in His Official Capacity
as the Director of the Office of Defense Trade Controls Policy Division;
SARAH J. HEIDEMA, Individually and in Her Official Capacity as the
Division Chief, Regulatory and Multilateral Affairs, Office of Defense Trade
Controls Policy; GLENN SMITH, Individually and in His Official Capacity as
the Senior Advisor, Office of Defense Trade Controls,

Defendants - Appellees

Appeal from the United States District Court
for the Western District of Texas

Before DAVIS, JONES, and GRAVES, Circuit Judges.

W. EUGENE DAVIS, Circuit Judge:

Plaintiffs-Appellants Defense Distributed and Second Amendment
Foundation, Inc. have sued Defendants-Appellees, the United States

No. 15-50759

Department of State, the Secretary of State, the DDTC, and various agency employees (collectively, the “State Department”), seeking to enjoin enforcement of certain laws governing the export of unclassified technical data relating to prohibited munitions. Because the district court concluded that the public interest in national security outweighs Plaintiffs-Appellants’ interest in protecting their constitutional rights, it denied a preliminary injunction, and they timely appealed. We conclude the district court did not abuse its discretion and therefore affirm.

I. Background

Defense Distributed is a nonprofit organization operated, in its own words, “for the purpose of promoting popular access to arms guaranteed by the United States Constitution” by “facilitating global access to, and the collaborative production of, information and knowledge related to the 3D printing of arms; and by publishing and distributing such information and knowledge on the Internet at no cost to the public.” Second Amendment Foundation, Inc. is a nonprofit devoted more generally to promoting Second Amendment rights.

Defense Distributed furthers its goals by creating computer files used to create weapons and weapon parts, including lower receivers for AR-15 rifles.¹ The lower receiver is the part of the firearm to which the other parts are attached. It is the only part of the rifle that is legally considered a firearm under federal law, and it ordinarily contains the serial number, which in part allows law enforcement to trace the weapon. Because the other gun parts, such as the barrel and magazine, are not legally considered firearms, they are not

¹ The district court capably summarized the facts in its memorandum opinion and order. *See Def. Distributed v. U.S. Dep’t of State*, 121 F. Supp. 3d 680, 686-88 (W.D. Tex. 2015). The facts set out in this opinion come largely from the district court’s opinion and the parties’ briefs.

No. 15-50759

regulated as such. Consequently, the purchase of a lower receiver is restricted and may require a background check or registration, while the other parts ordinarily may be purchased anonymously.

The law provides a loophole, however: anyone may make his or her own unserialized, untraceable lower receiver for personal use, though it is illegal to transfer such weapons in any way. Typically, this involves starting with an “80% lower receiver,” which is simply an unfinished piece of metal that looks quite a bit like a lower receiver but is not legally considered one and may therefore be bought and sold freely. It requires additional milling and other work to turn into a functional lower receiver. Typically this would involve using jigs (milling patterns), a drill press, other tools, and some degree of machining expertise to carefully complete the lower receiver. The result, combined with the other, unregulated gun parts, is an unserialized, untraceable rifle.

Defense Distributed’s innovation was to create computer files to allow people to easily produce their own weapons and weapon parts using relatively affordable and readily available equipment. Defense Distributed has explained the technologies as follows:

Three-dimensional (“3D”) printing technology allows a computer to “print” a physical object (as opposed to a two-dimensional image on paper). Today, 3D printers are sold at stores such as Home Depot and Best Buy, and the instructions for printing everything from jewelry to toys to car parts are shared and exchanged freely online at sites like GrabCAD.com and Thingiverse.com. Computer numeric control (“CNC”) milling, an older industrial technology, involves a computer directing the operation of a drill upon an object. 3D printing is “additive,” using raw materials, the printer constructs a new object. CNC milling is “subtractive,” carving something (more) useful from an existing object.

Both technologies require some instruction set or “recipe”—in the case of 3D printers, computer aided design (“CAD”) files, typically

No. 15-50759

in .stl format; for CNC machines, text files setting out coordinates and functions to direct a drill.²

Defense Distributed's files allow virtually anyone with access to a 3D printer to produce, among other things, Defense Distributed's single-shot plastic pistol called the Liberator and a fully functional plastic AR-15 lower receiver. In addition to 3D printing files, Defense Distributed also sells its own desktop CNC mill marketed as the Ghost Gunner, as well as metal 80% lower receivers. With CNC milling files supplied by Defense Distributed, Ghost Gunner operators are able to produce fully functional, unserialized, and untraceable metal AR-15 lower receivers in a largely automated fashion.

Everything discussed above is legal for United States citizens and will remain legal for United States citizens regardless of the outcome of this case. This case concerns Defense Distributed's desire to share all of its 3D printing and CNC milling files online, available without cost to anyone located anywhere in the world, free of regulatory restrictions.

Beginning in 2012, Defense Distributed posted online, for free download by anyone in the world, a number of computer files, including those for the Liberator pistol (the "Published Files"). On May 8, 2013, the State Department sent a letter to Defense Distributed requesting that it remove the files from the internet on the ground that sharing them in that manner violates certain laws. The district court summarized the relevant statutory and regulatory framework as follows:

Under the Arms Export Control Act ("AECA"), "the President is authorized to control the import and the export of defense articles and defense services" and to "promulgate regulations for the import and export of such articles and services." 22 U.S.C. § 2778(a)(1). The AECA imposes both civil and criminal penalties for violation of its provisions and implementing regulations, including

² Plaintiffs-Appellants' Original Brief on Appeal.

No. 15-50759

monetary fines and imprisonment. *Id.* § 2278(c) & (e). The President has delegated his authority to promulgate implementing regulations to the Secretary of State. Those regulations, the International Traffic in Arms Regulation (“ITAR”), are in turn administered by the DDTC [Directorate of Defense Trade Controls] and its employees. 22 C.F.R. 120.1(a).

The AECA directs that the “defense articles” designated under its terms constitute the United States “Munitions List.” 22 U.S.C. § 2778(a)(1). The Munitions List “is not a compendium of specific controlled items,” rather it is a “series of categories describing the kinds of items” qualifying as “defense articles.” *United States v. Zhen Zhou Wu*, 711 F.3d 1, 12 (1st Cir.) *cert. denied sub nom. Yufeng Wei v. United States*, —U.S. —, 134 S. Ct. 365, 187 L. Ed. 2d 160 (2013). Put another way, the Munitions List contains “attributes rather than names.” *United States v. Pulungan*, 569 F.3d 326, 328 (7th Cir. 2009) (explaining “an effort to enumerate each item would be futile,” as market is constantly changing). The term “defense articles” also specifically includes “technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in” the Munitions List. 22 C.F.R. § 120.6

A party unsure about whether a particular item is a “defense article” covered by the Munitions List may file a “commodity jurisdiction” request with the DDTC. *See* 22 C.F.R. § 120.4 (describing process). The regulations state the DDTC “will provide a preliminary response within 10 working days of receipt of a complete request for commodity jurisdiction.” *Id.* § 120.4(e). If a final determination is not provided after 45 days, “the applicant may request in writing to the Director, Office of Defense Trade Controls Policy that this determination be given expedited processing.” *Id.*³

In short, the State Department contended: (1) the Published Files were potentially related to ITAR-controlled “technical data” relating to items on the USML; (2) posting ITAR-controlled files on the internet for foreign nationals

³ *See Def. Distributed v. U.S. Dep’t of State*, 121 F. Supp. 3d 680, 687-88 (W.D. Tex. 2015).

No. 15-50759

to download constitutes “export”; and (3) Defense Distributed therefore must obtain prior approval from the State Department before “exporting” those files. Defense Distributed complied with the State Department’s request by taking down the Published Files and seeking commodity jurisdiction requests for them. It did eventually obtain approval to post some of the non-regulated files, but *all* of the Published Files continue to be shared online on third party sites like The Pirate Bay.

Since then, Defense Distributed has not posted any new files online. Instead, it is seeking prior approval from the State Department and/or DDTC before doing so, and it has not obtained such approval. The new files Defense Distributed seeks to share online include the CNC milling files required to produce an AR-15 lower receiver with the Ghost Gunner and various other 3D printed weapons or weapon parts.

District Court Proceedings

In the meantime, Defense Distributed and Second Amendment Foundation, Inc., sued the State Department, seeking to enjoin them from enforcing the regulations discussed above. Plaintiffs-Appellants argue that the State Department’s interpretation of the AECA, through the ITAR regulations, constitutes an unconstitutional prior restraint on protected First Amendment speech, to wit, the 3D printing and CNC milling files they seek to place online.⁴ They also claim violations of the Second and Fifth Amendments. Plaintiffs-Appellants’ challenges to the regulatory scheme are both facial and as applied, and they ultimately seek a declaration that no prepublication approval is

⁴ The State Department does not restrict the export of the Ghost Gunner machine itself or the user manual, only the specific CNC milling files used to produce the AR-15 lower receivers with it, as well as all 3D printing files used to produce prohibited weapons and weapon parts.

No. 15-50759

needed for privately generated unclassified information, whether or not that data may constitute “technical data” relating to items on the USML.

Plaintiffs-Appellants sought a preliminary injunction against the State Department, essentially seeking to have the district court suspend enforcement of ITAR’s prepublication approval requirement pending final resolution of this case. The district court denied the preliminary injunction, and Plaintiffs-Appellants timely filed this appeal. We review the denial of a preliminary injunction for abuse of discretion, but we review any questions of law de novo.⁵

To obtain a preliminary injunction, the applicant must show (1) a substantial likelihood that he will prevail on the merits, (2) a substantial threat that he will suffer irreparable injury if the injunction is not granted, (3) that his threatened injury outweighs the threatened harm to the party whom he seeks to enjoin, and (4) that granting the preliminary injunction will not disserve the public interest. “We have cautioned repeatedly that a preliminary injunction is an extraordinary remedy which should not be granted unless the party seeking it has ‘clearly carried the burden of persuasion’ on all four requirements.”⁶

We have long held that satisfying one requirement does not necessarily affect the analysis of the other requirements. In *Southern Monorail Co. v. Robbins & Myers, Inc.*, 666 F.2d 185 (5th Cir. Unit B 1982), for example, the district court had denied a preliminary injunction solely because it found that the movant, Robbins & Myers, failed to satisfy the balance of harm requirement. On appeal, Robbins & Myers argued that it had clearly shown a substantial likelihood of success on the merits, and satisfying that requirement should give rise to a presumption of irreparable harm and a presumption that the balance of harm tipped in its favor. We disagreed:

⁵ *PCI Transp., Inc. v. Fort Worth & W. R. Co.*, 418 F.3d 535, 545 (5th Cir. 2005) (footnotes omitted)

⁶ *Id.*

No. 15-50759

Because we dispose of this case on the balance of harm question, we need not decide and we express no views upon whether a presumption of irreparable injury as a matter of law is appropriate once a party demonstrates a substantial likelihood of success on the merits of an infringement claim. In other words, even assuming *arguendo* that Robbins & Myers has shown a substantial likelihood of success on the merits of its infringement claim and that irreparable injury should be presumed from such a showing (two issues not addressed by the district court in this case), we still uphold the district court's decision, which rested solely on the balance of harm factor. We agree that Robbins & Myers has failed to carry its burden of showing that the threatened harm to it from the advertisement outweighs the harm to Southern Monorail from the intercept. In addition, we expressly reject Robbins & Myers' suggestion that we adopt a rule that the balance of harm factor should be presumed in the movant's favor from a demonstration of a substantial likelihood of success on the merits of an infringement claim. Such a presumption of the balance of harm factor would not comport with the discretionary and equitable nature of the preliminary injunction in general and of the balance of harm factor in particular. *See Ideal Industries, Inc. v. Gardner Bender, Inc.*, 612 F.2d 1018, 1026 (7th Cir. 1979), *cert. denied*, 447 U.S. 924, 100 S. Ct. 3016, 65 L. Ed. 2d 1116 (1980) (district court obligated to weigh relative hardship to parties in relation to decision to grant or deny preliminary injunction, even when irreparable injury shown).⁷

The district court concluded that the preliminary injunction should be denied because Plaintiffs-Appellants failed to satisfy the balance of harm and public interest requirements, which do not concern the merits. (Assuming without deciding that Plaintiffs-Appellants have suffered the loss of First and Second Amendment freedoms, they have satisfied the irreparable harm requirement because any such loss, however intangible or limited in time,

⁷ *Id.* at 187-88.

No. 15-50759

constitutes irreparable injury.⁸) In extensive dicta comprising nearly two-thirds of its memorandum opinion, the district court also concluded that Plaintiffs-Appellants failed to show a likelihood of success on the merits. Plaintiffs-Appellants timely appealed, asserting essentially the same arguments on appeal. Plaintiffs-Appellants continue to bear the burden of persuasion on appeal.

Analysis

Because the district court held that Plaintiffs-Appellants only satisfied the irreparable harm requirement, they may obtain relief on appeal only if they show that the district court abused its discretion on all three of the other requirements. The district court denied the preliminary injunction based on its finding that Plaintiffs-Appellants failed to meet the two non-merits requirements by showing that (a) the threatened injury to them outweighs the threatened harm to the State Department, and (b) granting the preliminary injunction will not disserve the public interest. The court only addressed the likelihood of success on the merits as an additional reason for denying the injunction. Because we conclude the district court did not abuse its discretion on its non-merits findings, we decline to address the merits requirement.

The crux of the district court's decision is essentially its finding that the government's exceptionally strong interest in national defense and national security outweighs Plaintiffs-Appellants' very strong constitutional rights under these circumstances. Before the district court, as on appeal, Plaintiffs-Appellants failed to give *any* weight to the public interest in national defense and national security, as the district court noted:

⁸ See *Def. Distributed*, 121 F. Supp. 3d at 689 (citing *Elrod v. Burns*, 427 U.S. 347, 373, 96 S. Ct. 2673, 49 L. Ed. 2d 547 (1976); *Palmer v. Waxahachie Indep. Sch. Dist.*, 579 F.3d 502, 506 (5th Cir. 2009); *Ezell v. City of Chicago*, 651 F.3d 684, 699 (7th Cir. 2011)).

No. 15-50759

Plaintiffs rather summarily assert the balance of interests tilts in their favor because “[I]t is always in the public interest to prevent the violation of a party’s constitutional rights.” *Awad v. Ziriax*, 670 F.3d 1111, 1132 (10th Cir. 2012); *see also Jackson Women’s Health Org. v. Currier*, 760 F.3d 448, 458 n. 9 (5th Cir. 2014) (district court did not abuse its discretion in finding injunction would not disserve public interest because it will prevent constitutional deprivations).⁹

Ordinarily, of course, the protection of constitutional rights *would* be the highest public interest at issue in a case. That is not necessarily true here, however, because the State Department has asserted a very strong public interest in national defense and national security. Indeed, the State Department’s stated interest in preventing foreign nationals—including all manner of enemies of this country—from obtaining technical data on how to produce weapons and weapon parts is not merely tangentially related to national defense and national security; it lies squarely within that interest.

In the State Department’s interpretation, its ITAR regulations directly flow from the AECA and are the only thing preventing Defense Distributed from “exporting” to foreign nationals (by posting online) prohibited technical data pertaining to items on the USML. Plaintiffs-Appellants disagree with the State Department’s interpretation, but that question goes to the merits.

Because Plaintiffs-Appellants’ interest in their constitutional rights and the State Department’s interest in national defense and national security are both public interests, the district court observed that “[i]n this case, the inquiry [on these two requirements] essentially collapses.”¹⁰ It reasoned:

While Plaintiffs’ assertion of a public interest in protection of constitutional rights is well-taken, it fails to consider the public’s keen interest in restricting the export of defense articles. *See Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 24–25, 129 S.

⁹ *Id.* at 689.

¹⁰ *Id.*

No. 15-50759

Ct. 365, 172 L. Ed. 2d 249 (2008) (discussing failure of district court to consider injunction’s adverse impact on public interest in national defense); *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 826 (2nd Cir. 2015) (characterizing maintenance of national security as “public interest of the highest order”). It also fails to account for the interest—and authority—of the President and Congress in matters of foreign policy and export. *See Haig v. Agee*, 453 U.S. 280, 292, 101 S. Ct. 2766, 69 L. Ed. 2d 640 (1981) (matters relating to conduct of foreign relations “are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference”); *United States v. Pink*, 315 U.S. 203, 222–23, 62 S. Ct. 552, 86 L. Ed. 796 (1942) (conduct of foreign relations “is committed by the Constitution to the political departments of the Federal Government”); *Spectrum Stores, Inc. v. Citgo Petroleum Corp.*, 632 F.3d 938, 950 (5th Cir. 2011) (matters implicating foreign relations and military affairs generally beyond authority of court’s adjudicative powers).

As to Plaintiff’s second contention, that an injunction would not bar Defendants from controlling the export of classified information, it is significant that Plaintiffs maintain the posting of files on the Internet for free download does not constitute “export” for the purposes of the AECA and ITAR. But Defendants clearly believe to the contrary. Thus, Plaintiffs’ contention that the grant of an injunction permitting them to post files that Defendants contend are governed by the AECA and ITAR would not bar Defendants from controlling “export” of such materials stand in sharp [contrast] to Defendants’ assertion of the public interest. The Court thus does not believe Plaintiffs have met their burden as to the final two prongs necessary for granting Plaintiffs a preliminary injunction. Nonetheless, in an abundance of caution, the Court will turn to the core of Plaintiffs’ motion for a preliminary injunction, whether they have shown a likelihood of success on their claims[.]¹¹

Plaintiffs-Appellants suggest the district court disregarded their paramount interest in protecting their constitutional rights. That is not so. The district court’s decision was based not on discounting Plaintiffs-Appellants’

¹¹ *Id.* at 689-90.

No. 15-50759

interest but rather on finding that the public interest in national defense and national security is stronger here, and the harm to the government is greater than the harm to Plaintiffs-Appellants. We cannot say the district court abused its discretion on these facts.

Because both public interests asserted here are strong, we find it most helpful to focus on the balance of harm requirement, which looks to the relative harm to both parties if the injunction is granted or denied. If we affirm the district court's denial, but Plaintiffs-Appellants eventually prove they are entitled to a permanent injunction, their constitutional rights will have been violated in the meantime, but only temporarily. Plaintiffs-Appellants argue that this result is absurd because the Published Files are already available through third party websites such as the Pirate Bay, but granting the preliminary injunction sought by Plaintiffs-Appellants would allow them to share online not only the Published Files but also any new, previously unpublished files. That leads us to the other side of the balance of harm inquiry.

If we reverse the district court's denial and instead grant the preliminary injunction, Plaintiffs-Appellants would legally be permitted to post on the internet as many 3D printing and CNC milling files as they wish, including the Ghost Gunner CNC milling files for producing AR-15 lower receivers and additional 3D-printed weapons and weapon parts. Even if Plaintiffs-Appellants eventually fail to obtain a permanent injunction, the files posted in the interim would remain online essentially forever, hosted by foreign websites such as the Pirate Bay and freely available worldwide. That is not a far-fetched hypothetical: the initial Published Files are still available on such sites, and Plaintiffs-Appellants have indicated they will share additional, previously unreleased files as soon as they are permitted to do so. Because those files would never go away, a preliminary injunction would function, in effect, as a

No. 15-50759

permanent injunction as to all files released in the interim. Thus, the national defense and national security interest would be harmed forever. The fact that national security might be permanently harmed while Plaintiffs-Appellants' constitutional rights might be temporarily harmed strongly supports our conclusion that the district court did not abuse its discretion in weighing the balance in favor of national defense and national security.

In sum, we conclude that the district court did not abuse its discretion in denying Plaintiffs-Appellants' preliminary injunction based on their failure to carry their burden of persuasion on two of the three non-merits requirements for preliminary injunctive relief, namely the balance of harm and the public interest. We therefore affirm the district court's denial and decline to reach the question of whether Plaintiffs-Appellants have demonstrated a substantial likelihood of success on the merits.¹²

¹² The dissent disagrees with this opinion's conclusion that the balance of harm and public interest factors favor the State Department such that Plaintiffs-Appellants' likelihood of success on the merits could not change the outcome. The dissent argues that we "should have held that the domestic internet publication" of the technical data at issue presents no "immediate danger to national security, especially in light of the fact that many of these files are now widely available over the Internet and that the world is awash with small arms."

We note the following: (1) If Plaintiffs-Appellants' publication on the Internet were truly domestic, i.e., limited to United States citizens, there is no question that it would be legal. The question presented in this case is whether Plaintiffs-Appellants may place such files on the Internet for unrestricted worldwide download. (2) This case does not concern only the files that Plaintiffs-Appellants previously made available online. Plaintiffs-Appellants have indicated their intent to make many more files available for download as soon as they are legally allowed to do so. Thus, the bulk of the potential harm has not yet been done but could be if Plaintiffs-Appellants obtain a preliminary injunction that is later determined to have been erroneously granted. (3) The world may be "awash with small arms," but it is not yet awash with the ability to make untraceable firearms anywhere with virtually no technical skill. For these reasons and the ones we set out above, we remain convinced that the potential permanent harm to the State Department's strong national security interest outweighs the potential temporary harm to Plaintiffs-Appellants' strong First Amendment interest.

As to the dissent's extensive discussion of Plaintiffs-Appellants' likelihood of success on the merits of the First Amendment issue, we take no position. Even a First Amendment violation does not necessarily trump the government's interest in national defense. We simply hold that Plaintiffs-Appellants have not carried their burden on two of the four requirements for a preliminary injunction: the balance of harm and the public interest.

No. 15-50759

We are mindful of the fact that the parties and the amici curiae in this case focused on the merits, and understandably so. This case presents a number of novel legal questions, including whether the 3D printing and/or CNC milling files at issue here may constitute protected speech under the First Amendment, the level of scrutiny applicable to the statutory and regulatory scheme here, whether posting files online for unrestricted download may constitute “export,” and whether the ITAR regulations establish an impermissible prior restraint scheme. These are difficult questions, and we take no position on the ultimate outcome other than to agree with the district court that it is not yet time to address the merits.

On remand, the district court eventually will have to address the merits, and it will be able to do so with the benefit of a more fully developed record. The amicus briefs submitted in this case were very helpful and almost all supported Plaintiffs-Appellants’ general position. Given the importance of the issues presented, we may only hope that amici continue to provide input into the broader implications of this dispute.

Conclusion

For the reasons set out above, we conclude that the district court did not abuse its discretion by denying the preliminary injunction on the non-merits requirements. AFFIRMED.

No. 15-50759

JONES, Circuit Judge, dissenting:

This case poses starkly the question of the national government’s power to impose a prior restraint on the publication of lawful, unclassified, not-otherwise-restricted technical data to the Internet under the guise of regulating the “export” of “defense articles.” I dissent from this court’s failure to treat the issues raised before us with the seriousness that direct abridgements of free speech demand.

I.

From late 2012 to early 2013, plaintiff Defense Distributed posted on the Internet, free of charge, technical information including computer assisted design files (CAD files) about gun-related items including a trigger guard, two receivers, an ArmaLite Rifle-15 magazine,¹ and a handgun named “The Liberator.” None of the published information was illegal, classified for national security purposes, or subject to contractual or other distribution restrictions. In these respects the information was no different from technical data available through multiple Internet sources from widely diverse publishers. From scientific discussions to popular mechanical publications to personal blog sites, information about lethal devices of all sorts, or modifications to commercially manufactured firearms and explosives, is readily available on the Internet.

What distinguished Defense Distributed’s information at that time, however, was its computer files designed for 3D printer technology that could be used to “print” parts and manufacture, with the proper equipment and know-how, a largely plastic single-shot handgun. The Liberator technology

¹ The ArmaLite Rifle, design 15 is rifle platform commonly abbreviated AR-15, a registered trademark of Colt’s Inc. AR-15, Registration No. 0,825,581.

No. 15-50759

drew considerable press attention² and the relevant files were downloaded “hundreds of thousands of times.” In May 2013, Defense Distributed received a warning letter from the U.S. State Department stating in pertinent part:

DDTC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEFCAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

Pursuant to §127.1 of the ITAR, it is unlawful to export any defense article or technical data for which a license or written approval is required without first obtaining the required authorization from the DDTC. Please note that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is considered an export under §120.17 of the ITAR.

The letter then advised Defense Distributed that it must “remove [its information] from public access” immediately, pending its prompt request for and receipt of approval from DDTC.

In a nearly forty-year history of munitions “export” controls, the State Department had never sought enforcement against the posting of any kind of files on the Internet. Because violations of the cited regulations carry severe civil and criminal penalties,³ Defense Distributed had no practical choice but to remove the information and seek approval to publish from DDTC. It took

² According to Defense Distributed, the Liberator files were covered, inter alia, by Forbes, CNN, NBC News, and the Wall Street Journal.

³ Fines may exceed a million dollars and imprisonment, for violations premised on specific intent to violate, up to twenty years. 28 U.S.C. § 2778(c); *United States v. Covarrubias*, 94 F.3d 172 (5th Cir. 1996).

No. 15-50759

the government entities two years to refuse to exempt most of the files from the licensing regime.

Defense Distributed filed suit in federal court to vindicate, inter alia, its First Amendment right to publish without prior restraint⁴ and sought the customary relief of a temporary injunction to renew publication. This appeal stems from the district court's denial of relief. Undoubtedly, the denial of a temporary injunction in this case will encourage the State Department to threaten and harass publishers of similar non-classified information. There is also little certainty that the government will confine its censorship to Internet publication. Yet my colleagues in the majority seem deaf to this imminent threat to protected speech. More precisely, they are willing to overlook it with a rote incantation of national security, an incantation belied by the facts here and nearly forty years of contrary Executive Branch pronouncements.

This preliminary injunction request deserved our utmost care and attention. Interference with First Amendment rights for any period of time, even for short periods, constitutes irreparable injury. *Elrod v. Burns*, 427 U.S. 347, 373, 96 S. Ct. 2673, 2690 (1976) (citing *New York Times Co. v. United States*, 403 U.S. 713, 91 S. Ct. 2140 (1971)); *Opulent Life Church v. City of Holly Springs, Miss.*, 697 F.3d 279, 295–97 (5th Cir. 2012). Defense Distributed has been denied publication rights for over three years. The district court, moreover, clearly erred in gauging the level of constitutional protection to which this speech is entitled: intermediate scrutiny is

⁴ To simplify discussion, I refer to Defense Distributed as the plaintiff, but it is joined in litigation by the Second Amendment Foundation, and its arguments are adopted and extended by numerous amici curiae. Believing that the deprivation of a merits opinion is most critical to Defense Distributed's First Amendment claim, I do not discuss the plaintiffs' other non-frivolous claims premised on ultra vires, the Second Amendment and procedural due process.

No. 15-50759

inappropriate for the content-based restriction at issue here. (Why the majority is unwilling to correct this obvious error for the sake of the lower court's getting it right on remand is a mystery).

The district court's mischaracterization of the standard of scrutiny fatally affected its approach to the remaining prongs of the test for preliminary injunctive relief. Without a proper assessment of plaintiff's likelihood of success on the merits—arguably the most important of the four factors necessary to grant a preliminary injunction, *Tesfamichael v. Gonzales*, 411 F.3d 169, 176 (5th Cir. 2005)—the district court's balancing of harms went awry.⁵ We should have had a panel discussion about the government's right to censor Defense Distributed's speech.

Since the majority are close to missing in action, and for the benefit of the district court on remand, I will explain why I conclude that the State Department's application of its "export" control regulations to this domestic Internet posting appears to violate the governing statute, represents an irrational interpretation of the regulations, and violates the First Amendment as a content-based regulation and a prior restraint.

⁵ See *Tex. v. Seatrail Int'l, S.A.*, 518 F.2d 175, 180 (5th Cir. 1975) ("none of the four prerequisites has a fixed quantitative value. Rather, a sliding scale is utilized, which takes into account the intensity of each in a given calculus."). *Southern Monorail Co. v. Robbins & Myers, Inc.*, 666 F.2d 185 (5th Cir. 1982), is the only case relied upon by the majority for the proposition that we may dispense with addressing the likelihood of success on the merits if we conclude that the parties have not satisfied one of the other elements of the test for granting a preliminary injunction. That case is distinguishable. First, *Southern Monorail* was a private action concerning trademark infringement, not a case involving a claim of the invasion of constitutional rights by the federal government. See *id.* at 185–86. Second, "the district court denied the injunction *solely* on the basis of the third factor, concerning the balance of harm." *Id.* at 186 (emphasis added). In this case, by contrast, the district court addressed each of the preliminary injunction factors, thus allowing us to consider its resolution of each factor.

No. 15-50759

II.

A. Regulatory Framework

The Arms Export Control Act of 1976 (“AECA”) authorizes the President to “control the import and the export of defense articles and defense services.” 22 U.S.C. § 2778(a)(1). The President “is authorized to designate those items which shall be considered as defense articles and defense services . . . and to promulgate regulations for the import and export of such articles and services.” *Id.* “The items so designated shall constitute the United States Munitions List.” *Id.* The statute does not define “export,” but “defense items” includes defense articles, defense services “and related technical data.” 22 U.S.C. § 2778(j)(4)(A).

In response to this directive, the State Department promulgated the International Traffic in Arms Regulations (“ITAR”), which contain the United States Munitions List (“USML”). 22 C.F.R. § 121.1. The USML enumerates a vast array of weaponry, ammunition, and military equipment including, for present purposes, “firearms,” defined as “[n]onautomatic and semi-automatic firearms to caliber .50 inclusive,” 22 C.F.R. § 121.1, Category I, item (a).

The USML also broadly designates “technical data” relating to firearms as subject to the ITAR. 22 C.F.R. § 121.1, Category I, item (i). “Technical data” encompass any information “which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles including “information in the form of blueprints, drawings, photographs, plans, instructions or documentation.” 22 C.F.R. § 120.10(a)(1).

Notably excepted from “technical data” is information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain.”

No. 15-50759

22 C.F.R. § 120.10(b). Further, the “public domain” covers “information which is published and which is generally accessible or available to the public” through newsstands, bookstores, public libraries, conferences, meetings, seminars, trade shows, and “fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community.” 22 C.F.R. § 120.11(a).⁶

Under the ITAR it is unlawful to “export or attempt to export from the United States any defense article or technical data” without first obtaining a license or written approval from the Directorate of Defense Trade Controls (“DDTC”), a division of the State Department. 22 C.F.R. § 127.1(a)(1). When Defense Distributed published technical data on the Internet, the State Department defined “export” broadly, as, *inter alia*, “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad.” 22 C.F.R. § 120.17(a)(4).⁷

⁶ This provision only appears to permit dissemination of information *already* in the public domain. Indeed, the State Department has explicitly taken the position in this litigation and in a June 2015 Notice of Proposed Rulemaking that an individual wishing to place technical data in the public domain must obtain State Department approval. 80 Fed. Reg. at 31,528. The State Department has proposed, but has not yet adopted, a rule to make this distinction more explicit. *See id.*

⁷ Effective September 1, 2016, however, the State Department has amended that provision, now defining an export as, “[r]eleasing or otherwise transferring technical data to a foreign person in the United States.” *Id.* § 120.17(a)(2); *see also* International Traffic in Arms: Revisions to Definition of Export and Related Definitions, 81 Fed. Reg. 35,611, 35,616 (June 3, 2016). Moreover, in June 2015, the State Department issued a Notice of Proposed Rulemaking, which proposed adding to the term “export” “[m]aking technical data available via a publicly available network (e.g., the Internet).” This, of course, is the open-ended definition of “export” urged by the State Department in this litigation. *See* International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain, 80 Fed. Reg. 31,525, 31,535 (proposed June 3, 2015). The Notice advised that the State Department intends to address that definition in a separate rulemaking and for now allows the “existing ITAR controls [to] remain in place.” 81 Fed. Reg. at 35,613.

No. 15-50759

In order to resolve doubts about whether an “export” is covered by ITAR, parties may request a “commodity jurisdiction” determination from the DDTC, which will determine each request on a “case-by-case basis,” 22 C.F.R. § 120.4(a), taking into account “the form and fit of the article; and [t]he function and performance capability of the article.” 22 C.F.R. § 120.4 (d)(2)(i)–(ii).

The commodity jurisdiction process could, in theory, be avoided if the particular export is exempt from the DDTC process. 22 C.F.R. § 125.4. As relevant here, “[t]echnical data approved for public release (i.e., unlimited distribution) by the cognizant U.S. Government department or agency or Office of Freedom of Information and Security Review” is exempt from the DDTC approval process. 22 C.F.R. § 125.4(b)(13). Under this rubric, the Defense Office of Prepublication and Security Review (“DOPSR”), housed in the Department of Defense’s Defense Technical Information Center, “is responsible for managing the Department of Defense security review program, [and] reviewing written materials both for public and controlled release.” Defense Office of Prepublication and Security Review (DOPSR), EXECUTIVE SERVS. DIRECTORATE ONLINE, <http://www.dtic.mil/whs/esd/osr/> (last visited Aug. 22, 2016). The plaintiff’s experience suggests that, in practice, DOPSR will not act on requests for exemptions concerning items not clearly subject to the ITAR until DDTC issues a commodity jurisdiction determination.

The DDTC is required to provide a final commodity jurisdiction determination within 45 days of a commodity jurisdiction request, but if it is not then resolved, an applicant may request expedited processing. 22 C.F.R. § 120.4(e). The DDTC has been criticized by the Government Accountability Office and the Office of Inspector General for routinely failing to meet deadlines. In this case, it took nearly two years for DDTC to rule on the

No. 15-50759

plaintiffs' commodity jurisdiction applications. Although an applicant may appeal an unfavorable commodity jurisdiction determination within the State Department, *Id.* § 120.4(g), Congress has excluded from judicial review the agency's discretionary decisions in "designat[ing] . . . items as defense articles or defense services." 22 U.S.C. § 2778(h); 22 C.F.R. § 128.1.⁸

Should the DDTC determine, as here, that technical data are subject to the ITAR, an "export" license is required before the information may be posted online. But the license may be denied whenever the State Department "deems such action to be in furtherance of world peace, the national security of the United States, or is otherwise advisable." 22 C.F.R. § 126.7(a)(1). There is a nominal 60-day deadline for a licensing decision, which is riddled with exceptions, and denial of an export license is expressly exempt from judicial review. *See* 22 C.F.R. § 128.1.

I would hardly deny that the Department of Justice has good grounds for prosecuting attempts to export weapons and military technology illegally to foreign actors. Previous prosecutions have targeted defendants, *e.g.*, who

⁸ While 22 U.S.C. § 2778 (h) withholds judicial review as noted, 22 C.F.R. § 128.1 purports more broadly to preclude judicial review over the Executive's implementation of the AECA under the Administrative Procedure Act. I would construe these provisions narrowly to avoid difficult questions that might arise were the Government to take the position that these provisions prevent judicial review for all claims, including those founded on the Constitution. *See Kirby Corp v. Pena*, 109 F.3d 258, 261 (5th Cir. 1997) ("There is a strong presumption that Congress intends there to be judicial review of administrative agency action . . . and the government bears a 'heavy burden' when arguing that Congress meant to withdraw all judicial review."); *Dart v. United States*, 848 F.2d 217, 221 (D.C. Cir. 1988) ("If the wording of a preclusion clause is less than absolute, the presumption of judicial review also favors a particular *category* of plaintiffs' claims."); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142 (2016) (Agency "shenanigans" are "properly reviewable . . . under the Administrative Procedure Act, which enables reviewing courts to set aside agency action that is contrary to constitutional right, in excess of statutory jurisdiction, or arbitrary [and] capricious.") (internal quotations omitted).

No. 15-50759

attempted to deliver WMD materials to North Korea, who sought to distribute drone and missile schematics to China, and who attempted to license chemical purchasing software to companies owned by the Iranian government.⁹ Defense Distributed agrees, moreover, that the Government may prosecute individuals who email classified technical data to foreign individuals or directly assist foreign actors with technical military advice. *See, e.g., United States v. Edler Industries, Inc.*, 579 F.2d 516 (9th Cir. 1978), construing prior version of AECA. Yet, as plaintiff points out, at the time that DDTC stifled Defense Distributed’s online posting, there were no publicly known enforcement actions in which the State Department purported to require export licenses or prior approval for the domestic posting of lawful, unclassified, not-otherwise-restricted information on the Internet.

While Defense Distributed has been mired in this thicket of regulation, the CAD files that it published continue to be available to the international public to this day on websites such as the Pirate Bay. Moreover, technology has not stood still: design files are now available on the Internet for six- and eight-shot handguns that can be produced with 3D printing largely out of plastic materials. *See, e.g.,* Scott J. Grunewald, “The World’s First Fully Printed Revolver is Here”, 3DPrintBoard.com (Nov. 23, 2015) (site visited 9/14/2016).

B. Discussion

As applied to Defense Distributed’s publication of technical data, the State Department’s prepublication approval and license scheme lacks

⁹ *See* DEPARTMENT OF JUSTICE, SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES (*January 2009 to the present: updated August 12, 2015*) 3, 11, 86 (2015), available at <https://www.pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf>.

No. 15-50759

statutory and regulatory authorization and invades the plaintiffs First Amendment rights because it is both a content-based regulation that fails strict scrutiny and an unconstitutional prior restraint on protected speech.¹⁰

1. The Statute and its Regulatory Interpretation.

Whether AECA itself, concerned with the “export” of defense article related technical data, authorizes prepublication censorship of domestic publications on the Internet is at least doubtful. Further, construing the State Department’s regulations for such a purpose renders them incoherent and unreasonable.

It is necessary first to analyze the statute under which the State Department presumed to enact its regulations and, under the first prong of *Chevron* analysis, what the statute means.¹¹ The term “export” is not defined in the AECA, is not a term of legal art, and is not ambiguous. Under standard canons of statutory construction, “export” should bear its most common meaning. According to dictionaries, the verb “export” means “to ship (commodities) to other countries or places for sale, exchange, etc.” *United States v. Ehsam*, 163 F.3d 858, 859 (4th Cir. 1998) (citing *The Random House Dictionary of the English Language* 682 (2d ed.1987)); *Export*, *Black’s Law Dictionary* (10th ed. 2014) (“To send, take, or carry (a good or commodity) out of the country; to transport (merchandise) from one country to another in the course of trade”); *United States v. Dien Duc Huynh*, 246 F.3d 734, 741 (5th Cir. 2001) (“Exportation occurs when the goods are shipped to another country”).

¹⁰ For simplicity only, I do not here address plaintiffs’ vagueness claim.

¹¹ It is hard to say whether the State Department’s interpretation of AECA should be analyzed under *Chevron*, *U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842, 104 S. Ct. 2778, 2781 (1984) or *United States v. Mead Corp.*, 533 U.S. 218, 227–28, 121 S. Ct. 2164, 2171–72 (2001). I refer to *Chevron* analysis *arguendo* because it captures both the statute and the reasonableness of the regulations.

No. 15-50759

As the court explained in *Ehsam*, which interpreted a Presidential proclamation banning “exportation” of goods or technology to Iran, “[t]hese definitions vary in specificity, but all make clear that exportation involves the transit of goods from one country to another for the purpose of trade.” *Id.* See also *Swan v. Finch Co. v. United States*, 190 U.S. 143, 145 (1903) (the “legal notion...of exportation is a severance of goods from the mass of things belonging to this country with an intention of uniting them to things belonging to some foreign country or another”). As against a claim that the rule of lenity should apply, the *Ehsam* court explicitly held that “export” is unambiguous. *Id.* at 859–60

Given this construction of “export” by a fellow circuit court, we have no reason to hold that Congress deviated from the term’s plain meaning, particularly so significantly as to encompass the domestic publication on the Internet, without charge and therefore without any “trade,” of lawful, nonclassified, nonrestricted information. “Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.” *King v. Burwell*, 135 S. Ct. 2480, 2495 (2015) (internal quotation omitted). Pursuant to *Chevron*, where the meaning of a statute is plain, a federal agency has no warrant to act beyond the authority delegated by Congress. *Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842–43, 104 S. Ct. 2778, 2781 (1984). The State Department’s briefing makes no effort to address the statutory language, which must be read in light of established case law and the term’s ordinary meaning and the rule of constitutional avoidance.

This determination of the meaning of “export” under *Chevron* step one would normally resolve the case. For the sake of argument, however, it is also clear that the State Department regulations fail the second step as well. Under

No. 15-50759

the second step of *Chevron* analysis, they may be upheld only if they represent a “reasonable” construction of the statute. *Chevron*, 467 U.S. at 844, 104 S. Ct. at 2782. Defense Distributed and its amici challenge the regulations’ interpretation of “export” and the “public domain” exception to the definition of “technical data.” Although the majority opinion adopts the State Department’s litigating position that “export” refers only to publication on the Internet, where the information will inevitably be accessible to foreign actors, the warning letter to Defense Distributed cited the exact, far broader regulatory definition: “export” means “disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad.” There is embedded ambiguity, and disturbing breadth, in the State Department’s discretion to prevent the dissemination (without an “export” license) of lawful, non-classified technical data to foreign persons within the U.S. The regulation on its face, as applied to Defense Distributed, goes far beyond the proper statutory definition of “export.”

Even if “export” in AECA could bear a more capacious interpretation, applying the State Department’s regulatory interpretation to the non-transactional publication of Defense Distributed’s files on the Internet is unreasonable. In terms of the regulations themselves, how this expansive definition of “export” interacts with the “public domain” exception is unclear at best. If any dissemination of information bearing on USML technical data to foreign persons within the U.S. is potentially an “export,” then facilitating domestic publication of such information free of charge can never satisfy the “public domain” exception because newspapers, libraries, magazines, conferences, etc. may all be accessed by foreign persons. The State Department’s *ipse dixit* that “export” is consistent with its own “public domain” regulation is incoherent and unreasonable. Even if these regulations are

No. 15-50759

consistent, however, attempting to exclude the Internet from the “public domain,” whose definition does not currently refer to the Internet, is irrational and absurd. The Internet has become the quintessential “public domain.” The State Department cannot have it both ways, broadly defining “export” to cover non-transactional publication within the U.S. while solely and arbitrarily excluding from the “public domain” exception the Internet publication of Defense Distributed’s technical data.

The root of the problem is that the State Department’s litigating position and its regulations put more weight on “export” than any reasonable construction of the statute will bear. “Export” and “publication” are functionally different concepts. *Cf. Bond*, 134 S. Ct. at 2090 (“[s]aying that a person ‘used a chemical weapon conveys a very different idea than saying the person ‘used a chemical in a way that caused some harm.’” Not only does the State Department fail to justify according its interpretation *Chevron* deference, but the doctrine of constitutional avoidance establishes that *Chevron* deference would be inappropriate anyway. That doctrine provides that “where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress.” *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988); *see also id.* at 574–75 (stating that although the agency interpretation at issue “would normally be entitled to deference,” “[a]nother rule of statutory construction [constitutional avoidance]. . . is pertinent here”); *see also Solid Waste Agency of N. Cook County v. United States Army Corps of Eng’rs*, 531 U.S. 159, 174 (2001) (“We thus read the statute as written to avoid the significant constitutional and federalism questions raised by respondents’ interpretation, and therefore reject the

No. 15-50759

request for administrative deference.”). As the following constitutional discussion shows, the Executive Branch has consistently recognized the conceptual difference between “export” and “publication”, and its constitutional significance, throughout the forty-year history of the AECA. It is only the novel threatened enforcement in this case that brings to the fore the serious problems of censorship that courts are bound to address.

2. The First Amendment—Content-based speech restriction.

“Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves they are narrowly tailored to serve compelling state interests.” *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2226 (2015). “Government regulation of speech is content-based if a law applies to particular speech because of the topic discussed or the idea or message expressed.” *Id.* at 2227. “A speech regulation targeted at specific subject matter is content based even if it does not discriminate among viewpoints within that subject matter:” consequently, even a viewpoint neutral law can be content-based. *Id.* at 2230. “Strict scrutiny applies either when a law is content based on its face or when the purpose and justification for the law are content based.” *Id.* at 2228.

The prepublication review scheme at issue here would require government approval and/or licensing of any domestic publication on the Internet of lawful, non-classified “technical information” related to “firearms” solely because a foreign national might view the posting. As applied to the publication of Defense Distributed’s files, this process is a content-based restriction on the petitioners’ domestic speech “because of the topic discussed.” *Reed*, 135 S. Ct. at 2227. Particularly relevant to this case is *Holder v. Humanitarian Law Proj.*, 561 U.S. 1, 27–28, 130 S. Ct. 2705, 2723–24 (2010),

No. 15-50759

in which the Supreme Court held that as applied, a criminal statute forbidding the provision of material support and resources to designated terrorist organizations was content based and required strict scrutiny review. The Court there rejected the government's assertion that although the plaintiffs were going to provide legal training and political advocacy to Mideast terrorist organizations, the statute criminalized "conduct" and only incidentally affected "speech." Rejecting this incidental burden argument for intermediate scrutiny review, the Court stated the obvious: "[p]laintiffs want to speak to the PKK and the LTTE, and whether they may do so under §2239B depends on what they say:" if their speech concerns "specialized knowledge" it is barred, but it "if it imparts only general or unspecialized knowledge" it is permissible). *Humanitarian Law Proj.*, 130 S. Ct. at 2724.

The State Department barely disputes that computer-related files and other technical data are speech protected by the First Amendment. See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 445–49 (2d Cir. 2001) (discussing level of scrutiny owed for "speech" in the form of a decryption computer program). There are CAD files on the Internet and designs, drawings, and technical information about myriad items—jewelry, kitchen supplies, model airplanes, or clothing, for example—that are of no interest to the State Department. Only because Defense Distributed posted technical data referring to firearms covered generically by the USML does the government purport to require prepublication approval or licensing. This is pure content-based regulation.¹²

¹² The Ninth Circuit held in *United States v. Mak* that "the AECA and its implementing regulations are content-neutral" because "[t]he purpose of the AECA does not rest upon disagreement with the message conveyed," and because "ITAR defines the technical data based on its *function* and not its viewpoint." 683 F.3d 1126, 1134–35 (9th Cir. 2012). *Mak* is distinguishable for a number of reasons. First, the defendant was prosecuted for

No. 15-50759

The Government’s argument that its regulatory scheme is content-neutral because it is focused on curbing harmful secondary effects rather than Defense Distributed’s primary speech is unpersuasive. The Supreme Court explained this distinction in *Boos v. Barry*, which overturned an ordinance restricting criticism of foreign governments near their embassies because it “focus[es] on the direct impact of speech on its audience.” Secondary effects of speech, as the Court understood, include “congestion, [] interference with ingress or egress, [] visual clutter, or [] the need to protect the security of embassies”, which are the kind of regulations that underlie *Renton v. Playtime Theaters*. 485 U.S. 312, 321, 108 S. Ct. 1157, 1163–64 (1988). Similarly, the regulation of speech here is focused on the “direct impact of speech on its audience” because the government seeks to prevent certain listeners—foreign nationals—from using the speech about firearms to create guns.

The State Department also asserts that the ITAR regulatory scheme is not content-based because the information here at issue is “functional,” that is, that downloading the Defense Distributed files directly enables the creation of 3D printed gun and gun components “at the push of a button.” This argument is flawed factually and legally. First, more than CAD (or CNC) files are involved in the information sought to be regulated by the State Department:

attempting to export to the People’s Republic of China sensitive submarine technology loaded on unauthorized CDs and was arrested when he was carrying them aboard an international flight. Second, *Mak* was decided before *Reed* where the Supreme Court counseled that “[s]ome facial distinctions based on a message are obvious, defining regulated speech by particular subject matter, and others are more subtle, defining regulated speech by its function or purpose. Both are distinctions drawn based on the message a speaker conveys, and, therefore, are subject to strict scrutiny.” 135 S. Ct. at 2230. Third, even if the case is analyzed as a content-based restriction, Mak’s prosecution falls comfortably within the traditional understanding of “export.” The government’s heightened interest in national security is evident, and the Court required the government to prove beyond a reasonable doubt that the technical information he was carrying was not in the public domain.

No. 15-50759

its warning letter to Defense Distributed identified both “files” and “technical data,” which include design drawings, rendered images, and written manufacturing instructions. Second, CAD files do not “direct a computer” to do anything. As the amicus Electronic Frontier Foundation explains, “[T]o create a physical object based on a CAD file, a third party must supply additional software to read these files and translate them into the motions of a 3D print head, the 3D printer itself, and the necessary physical materials.” The person must provide know-how, tools and materials to assemble the printed components, *e.g.* treating some parts of the Liberator with acetone to render them functional. In effect, the “functionality” of CAD files differs only in degree from that of blueprints. Legally, this argument is an attempt to fit within the *Corley* case, referenced above, which concerned a computer program that by itself provided a “key” to open otherwise copyright-restricted online materials; those facts are far afield from the technical data speech at issue here. *Corley*, 273 F.3d at 449–55.

Because the regulation of Defense Distributed’s speech is content-based, it is necessary to apply strict scrutiny. The district court erred in applying the lower intermediate scrutiny standard. I would not dispute that the government has a compelling interest in enforcing the AECA to regulate the export of arms and technical data governed by the USML. The critical issue is instead whether the government’s prepublication approval scheme is narrowly tailored to achieve that end. A regulation is not narrowly tailored if it is “significantly overinclusive.” *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 121, 112 S. Ct. 501, 511 (1991).

“[S]ignificantly overinclusive,” however, aptly describes the Government’s breathtaking assertion of prepublication review and licensing authority as applied in this case. To prevent foreign nationals from accessing

No. 15-50759

technical data relating to USML-covered firearms, the government seeks to require all domestic posting on the Internet of “technical data” to be pre-approved or licensed by the DDTC. No matter that citizens have no intention of assisting foreign enemies directly, communications about firearms on webpages or blogs must be subject to prior approval on the theory that a foreign national *might* come across the speech. This flies in the face of *Humanitarian Law Project*. Although a statute prohibiting the provision of “material support and resources” to designated terrorist groups did not violate First Amendment rights where plaintiffs intended to *directly* assist specific terrorist organizations, the Court “in no way suggest[ed] that a regulation of independent speech would pass constitutional muster, even if the Government were to show that such speech benefits foreign terrorist organizations...[or] that Congress could extend the same prohibition on material support at issue here to domestic organizations.” 561 U.S. at 36–39, 130 S. Ct. at 2729–30. The State Department’s ITAR regulations, as sought to be applied here, plainly sweep in and would control a vast amount of perfectly lawful speech.

Two exceptions to the regulations do not eliminate the problem of overinclusiveness. First, general scientific, mechanical, or engineering principles taught in schools is deemed exempt from ITAR as information in the public domain. This exception does not, however, appear to save from potential regulation and licensing the amateur gunsmith or hobby shooter who discusses technical information about the construction of firearms on an Internet webpage. Any information so shared is not necessarily “general scientific, mechanical, or engineering principles taught in schools.” Underscoring this problem, at oral argument the government would not definitively answer whether the State Department would purport to regulate the posting of such

No. 15-50759

unclassified technical data that appeared in library books or magazines like Popular Mechanics.

Second, the State Department has taken the position in this litigation that the “public domain” exception applies only to information *already* in the public domain. Its interpretation of the technical data regulations would permit the DDTC to stifle online discussion of any innovations related to USML-covered firearms because new information would, by definition, not be in the public domain already. Amicus Reporters Committee for Freedom of the Press and the Thomas Jefferson Center for the Protection of Free Expression correctly expresses fear about journalists’ ability to report, without DDTC approval, on the latest technological innovations related to any items covered by the USML.

Lest this concern of overinclusiveness be perceived as hyperbole, consider that in 2013, CNET published an article containing an unredacted copy of a document detailing performance requirements for unmanned U.S. military surveillance drones.¹³ Should CNET have applied for approval or a license from the DDTC prior to publication? The State Department’s interpretation of the regulations could lead to that conclusion. See 22 C.F.R. § 121.1, Category VIII, item (i) (technical data related to aircraft and related articles). The USML-related technical discussed there (1) were “exported” because of their availability to foreign persons by publication on the Internet, and (2) the “public domain” exception would be of no avail since the information had not been in the public domain (narrowly defined to exclude

¹³ See Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET (Mar. 2, 2013, 11:30 AM), <http://www.cnet.com/news/dhs-built-domestic-surveillance-tech-into-predator-drones/>.

No. 15-50759

the Internet) before publication in the CNET article. On the Government's theory, journalists could be subject to the ITAR for posting articles online.

The State Department also asserts that, somehow, the information published by Defense Distributed would have survived regulatory scrutiny (query before or after submission to DDTC?) if the company had "verified the citizenship of those interested in the files, or by any other means adequate to ensure that the files are not disseminated to foreign nationals." Government brief at 20. Whatever this means, it is a ludicrous attempt to narrow the ambit of its regulation of Internet publications. Everyone knows that personally identifying information can be fabricated on electronic media. Equally troubling, if the State Department truly means what it says in brief about screening out foreign nationals, then the "public domain" exception becomes useless when applied to media like print publications and TV or to gatherings open to the public.

In sum, it is not at all clear that the State Department has *any* concern for the First Amendment rights of the American public and press. Indeed, the State Department turns freedom of speech on its head by asserting, "The possibility that an Internet site could also be used to distribute the technical data domestically does not alter the analysis...." The Government bears the burden to show that its regulation is narrowly tailored to suit a compelling interest. It is not the public's burden to prove their right to discuss lawful, non-classified, non-restricted technical data. As applied to Defense Distributed's online publication, these overinclusive regulations cannot be narrowly tailored and fail strict scrutiny.

3. The First Amendment--Prior Restraint.

The Government's prepublication approval and licensing scheme also fails to pass constitutional muster because it effects a prior restraint on speech.

No. 15-50759

The classic description of a prior restraint is an “administrative [or] judicial order[] forbidding certain communications when issued in advance of the time that such communications are to occur.” *Catholic Leadership Coalition of Tex. v. Reisman*, 764 F.3d 409, 437 (5th Cir. 2014) (citing *Alexander v. United States*, 509 U.S. 544, 550, 113 S. Ct. 2766, 2771 (1993)). The State Department’s prepublication review scheme easily fits the mold.

Though not unconstitutional *per se*, any system of prior restraint bears a heavy presumption of unconstitutionality. *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 225, 110 S. Ct. 596, 604 (1990). Generally, speech licensing schemes must avoid two pitfalls. First the licensors must not exercise excessive discretion. *Catholic Leadership Coalition*, 764 F.3d at 437 (citing *Lakewood v. Plain Dealer Publ’g Co.*, 486 U.S. 750, 757, 108 S. Ct. 2138, 2144 (1988)). “[N]arrowly drawn, reasonable and definite standards” should guide the licensor in order to avoid “unbridled discretion” that might permit the official to “encourag[e] some views and discourag[e] others through the arbitrary application” of the regulation. *Forsyth Cty., Ga. v. Nationalist Movement*, 505 U.S. 123, 133, 112 S. Ct. 2395, 2402–03 (1992).

Second, content-based¹⁴ prior restraints must contain adequate procedural protections. The Supreme Court has requires three procedural safeguards against suppression of protected speech by a censorship board: (1) any restraint before judicial review occurs can be imposed for only a specified brief period of time during which the status quo is maintained; (2) prompt judicial review of a decision must be available; and (3) the censor must bear the burdens of going to court and providing the basis to suppress

¹⁴ As described above, the ITAR regulation of posting to the Internet technical data related to USML-covered firearms is content-based. Thus, it is subject to the procedural requirements set forth in *Freedman v. Maryland*.

No. 15-50759

the speech. *N.W. Enters. v. City of Houston*, 352 F.3d 162, 193–94 (5th Cir. 2003) (citing *Friedman v. Maryland*, 380 U.S. 51, 58–59, 85 S. Ct. 734, 739 (1965)). In sum, a court reviewing a system of prior restraint should examine “both the law’s procedural guarantees and the discretion given to law enforcement officials.” *G.K. Ltd. Travel v. City of Lake Oswego*, 436 F.3d 1064, 1082 (9th Cir. 2006); *see also East Brooks Books, Inc. v. Shelby Cty.*, 588 F.3d 360, 369 (6th Cir. 2009); *Weinberg v. City of Chi.*, 310 F.3d 1029, 1045 (7th Cir. 2002).

To the extent it embraces publication of non-classified, non-transactional, lawful technical data on the Internet, the Government’s scheme vests broad, unbridled discretion to make licensing decisions and lacks the requisite procedural protections. First, as explained above, the “export” regulations’ virtually unbounded coverage of USML-related technical data posted to the Internet, combined with the State Department’s deliberate ambiguity in what constitutes the “public domain,” renders application of ITAR regulations anything but “narrow, objective, and definite.” The stated standards do not guide the licensors to prevent unconstitutional prior restraints. *Shuttlesworth v. City of Birmingham*, 394 U.S. 147, 151, 89 S. Ct. 935, 938 (1969). The State Department’s brief actually touts the case-by-case nature of the determination whether to prevent Internet publication of technical data.¹⁵

In *City of Lakewood v. Plain Dealer Publishing Co.*, for example, the Supreme Court held that a city ordinance insufficiently tailored the Mayor’s

¹⁵ Compounding confusion, the ITAR grant broad discretion to DDTC to deny an export license if it “deems such action to be in furtherance of world peace, the national security or the foreign policy of the United States, *or is otherwise advisable*.” 22 C.F.R. § 126.7(a)(1) (emphasis added).

No. 15-50759

discretion to issue newspaper rack permits because “the ordinance itself contains no explicit limits on the mayor’s discretion” and “nothing in the law as written requires the mayor to do more than make the statement ‘it is not in the public interest’ when denying a permit application.” 486 U.S. at 769, 108 S. Ct. at 2150–51. Like the “illusory ‘constraints’” in *Lakewood*, *id.* at 769, the ITAR prepublication review scheme offers nothing but regulatory (or prosecutorial) discretion, as applied to the technical data at issue here, in lieu of objective standards. Reliance on the censor’s good faith alone, however, “is the very presumption that the doctrine forbidding unbridled discretion disallows.” *Id.* at 770. *Cf. Humanitarian Law Project*, 130 S. Ct. at 2728 (listing numerous ways in which Congress had exhibited sensitivity to First Amendment concerns by limiting and clarifying a statute’s application and “avoid[ing] any restriction on independent advocacy, or indeed any activities not directed to, coordinated with, or controlled by foreign terrorist groups”).

Just as troubling is the stark lack of the three required procedural protections in prior restraint cases. Where a commodity jurisdiction application is necessary, the alleged 45-day regulatory deadline for such determinations seems to be disregarded in practice; nearly two years elapsed between Defense Distributed’s initial request and a response from the DDTC. Further, the prescribed time limit on licensing decisions, 60 days, is not particularly brief. *See Teitel Film Corp. v. Cusak*, 390 U.S. 139, 141, 88 S. Ct. 754, 756 (1968).

More fundamentally, Congress has withheld judicial review of the State Department’s designation of items as defense articles or services. *See* 22 U.S.C. § 2778(h); 22 C.F.R. § 128.1 (precluding judicial view of the Executive’s implementation of the AECA under the APA). The withholding of judicial review alone should be fatal to the constitutionality of this prior restraint

No. 15-50759

scheme insofar as it involves the publication of unclassified, lawful technical data to the Internet. *See City of Littleton, Colo. v. Z.J. Gifts D-4, LLC*, 541 U.S. 774, 781, 124 S. Ct. 2219, 2224 (2004) (noting that the Court’s decision in *FW/PBS, Inc. v. City of Dallas*, interpreting *Freedman*’s “judicial review” safeguard, requires “a prompt judicial decision,” as well as prompt access to the courts). And where judicial review is thwarted, it can hardly be said that DDTC, as the would-be censor, can bear its burden to go to court and support its actions.

C. The Government’s Interest, Balancing the Interests

A brief discussion is necessary on the balancing of interests as it should have been done in light of the facts of this case. No one doubts the federal government’s paramount duty to protect the security of our nation or the Executive Branch’s expertise in matters of foreign relations. Yet the Executive’s mere incantation of “national security” and “foreign affairs” interests do not suffice to override constitutional rights. The Supreme Court has long declined to permit the unsupported invocation of “national security” to cloud the First Amendment implications of prior restraints. *See New York Times Co. v. United States*, 403 U.S. 713, 714, 91 S. Ct. 2140, 2141 (1971) (reversing the grant of an injunction precluding the *New York Times* and the *Washington Post* from publishing the Pentagon Papers, a classified study of United States involvement in Vietnam from 1945–1967); *id.* at 730 (Stewart, J., concurring) (noting that because he cannot say that disclosure of the Pentagon Papers “will surely result in direct, immediate, and irreparable damage to our Nation or its people,” publication may not be enjoined consonant with the First Amendment). Indeed, only the most exceptional and immediate of national security concerns allow a prior restraint on speech to remain in place:

No. 15-50759

the protection as to previous restraint is not absolutely unlimited. But the limitation has been recognized only in exceptional cases^[n]o one would question but that a government might prevent actual obstruction to its recruiting service or the publication of sailing dates of transports or the number and location of troops. On similar grounds, the primary requirements of decency may be enforced against obscene publications. The security of the community life may be protected against incitements to acts of violence and the overthrow by force of orderly government.

Near v. Minnesota ex rel. Olson, 283 U.S. 697, 716, 51 S. Ct. 625, 631 (1931); *cf. Haig v. Agee*, 453 U.S. 280, 306–08, 101 S. Ct. 2766, 2781–82 (1981) (holding that the Secretary of State’s revocation of Haig’s passport did not violate First Amendment rights because his actions exposing undercover CIA agents abroad threatened national security). No such exceptional circumstances have been presented in this case. Indeed, all that the majority can muster to support the government’s position here is that

the State Department’s stated interest in preventing foreign nationals—including manner of enemies of this country—from obtaining technical data on how to produce weapons and weapon parts is not merely tangentially related to national defense and national security; it lies squarely within that interest.

Neither the district court nor the State Department offers anything else.¹⁶ With that kind of reasoning, the State Department could wholly eliminate the “public domain” and “scholarly” exceptions to the ITAR and require pre-publication approval of all USML-related technical data. This is clearly not

¹⁶ The State Department notes the fear that a single-shot pistol undetectable by metal-sensitive devices could be used by terrorists. The Liberator, however, requires a metal firing pin.

No. 15-50759

what the Supreme Court held in the *Pentagon Papers* or *Near* cases. See generally L.A. Powe, Jr., *The H-Bomb Injunction*, 61 U.Colo.L.Rev. 55 (1990).

Without any evidence to the contrary, the court should have held that the domestic Internet publication of CAD files and other technical data for a 3D printer-enabled making of gun parts and the Liberator pistol presents no immediate danger to national security, especially in light of the fact that many of these files are now widely available over the Internet and that the world is awash with small arms.¹⁷

Further, the government's pro-censorship position in this case contradicts the express position held within the Executive Branch for the nearly forty-year existence of the AECA. The State Department's sudden turnabout severely undercuts its argument that prepublication review and licensing for the publication of unclassified technical data is justified by pressing national security concerns. Indeed, in the late 1970s and early 1980s, at the height of the Cold War, the Department of Justice's Office of Legal Counsel repeatedly offered written advice that a prepublication review process would raise significant constitutional questions and would likely constitute an impermissible prior restraint, particularly when applied to unclassified technical data disseminated by individuals who do not possess specific intent to deliver it to particular foreign nationals. Further, in a 1997 "Report on the Availability of Bombmaking Information," the Department of Justice observed the widespread availability of bombmaking instructions on the Internet, in

¹⁷ The Government also vaguely asserts that imposing a prior restraint upon the domestic publication of the technical data here is justified to protect foreign relations with other countries that have more restrictive firearms laws than the United States. Inflicting domestic speech censorship in pursuit of globalist foreign relations concerns (absent specific findings and prohibitions as in *Humanitarian Law Project*) is dangerous and unprecedented.

No. 15-50759

libraries, and in magazines. The Department of Justice then argued against government censorship, concluding that despite the distinct possibility that third parties can use bombmaking instructions to engage in illegal conduct, a statute “proscrib[ing] indiscriminately the dissemination of bombmaking information” would face First Amendment problems because the government may rarely prevent the dissemination of truthful information.¹⁸

With respect to the ITAR’s regulation of “technical data,” DDTC’s director has taken the position in litigation that the State Department “does not seek to regulate the *means* themselves by which information is placed in the public domain” and “does not review in advance scientific information to determine whether it may be offered for sale at newsstands and bookstores, through subscriptions, second-class mail, or made available at libraries open to the public, or distributed at a conference or seminar in the United States.” Second Declaration of William J. Lowell Department of State Office of Defense Trade Controls at 11, *Bernstein v. U.S. Dep’t of State*, 945 F. Supp. 1279 (N.D. Cal. 1996). Moreover, he added, “the regulations are not applied to establish a prepublication review requirement for the general publication of scientific information in the United States.” *Id.*

Finally, the State Department’s invocation of unspecified national security concerns flatly contradicts its contention that while Defense Distributed’s very same technical data cannot be published on the Internet, they may be freely circulated within the U.S. at conferences, meetings, trade shows, in domestic print publications and in libraries. (Of course, as above noted, the Government’s sincerity on this point is subject to doubt, based on

¹⁸ DEPARTMENT OF JUSTICE, 1997 REPORT ON THE AVAILABILITY OF BOMBMAKING INFORMATION 3, 5–7, 19–29 (1997).

No. 15-50759

the determined ambiguity of its litigating position.) After all, if a foreign national were to attend a meeting or trade show, or visit the library and read a book with such information in it, under the Government's theory, the technical data would have been "exported" just like the Internet posts, because it was "[d]isclos[ed] (including oral or visual disclosure). . . to a foreign person . . . in the United States or abroad." *Id.* § 120.17(a)(4).

By refusing to address the plaintiffs' likelihood of success on the merits and relying solely on the Government's vague invocation of national security interests, the majority leave in place a preliminary injunction that degrades First Amendment protections and implicitly sanctions the State Department's tenuous and aggressive invasion of citizens' rights. The majority's non-decision here encourages case-by-case adjudication of prepublication review "requests" by the State Department that will chill the free exchange of ideas about whatever USML-related technical data the government chooses to call "novel," "functional," or "not within the public domain." It will foster further standardless exercises of discretion by DDTC censors.

Today's target is unclassified, lawful technical data about guns, which will impair discussion about a large swath of unclassified information about firearms and inhibit amateur gunsmiths as well as journalists. Tomorrow's targets may be drones, cybersecurity, or robotic devices, technical data for all of which may be implicated on the USML. This abdication of our decisionmaking responsibility toward the First Freedom is highly regrettable. I earnestly hope that the district court, on remand, will take the foregoing discussion to heart and relieve Defense Distributed of this censorship.

BILL OF COSTS

NOTE: The Bill of Costs is due in this office *within 14 days from the date of the opinion, See FED. R. APP. P. & 5TH CIR. R. 39.* Untimely bills of costs must be accompanied by a separate motion to file out of time, which the court may deny.

_____ v. _____ No. _____

The Clerk is requested to tax the following costs against: _____

COSTS TAXABLE UNDER Fed. R. App. P. & 5 th Cir. R. 39	REQUESTED				ALLOWED (If different from amount requested)			
	No. of Copies	Pages Per Copy	Cost per Page*	Total Cost	No. of Documents	Pages per Document	Cost per Page*	Total Cost
Docket Fee (\$500.00)								
Appendix or Record Excerpts								
Appellant's Brief								
Appellee's Brief								
Appellant's Reply Brief								
Other:								
Total \$					Costs are taxed in the amount of \$			

Costs are hereby taxed in the amount of \$ _____ this _____ day of _____.

State of _____
County of _____
By _____ Deputy Clerk
LYLE W. CAYCE, CLERK

I _____, do hereby swear under penalty of perjury that the services for which fees have been charged were incurred in this action and that the services for which fees have been charged were actually and necessarily performed. A copy of this Bill of Costs was this day mailed to opposing counsel, with postage fully prepaid thereon. This _____ day of _____.

(Signature)
Attorney for _____

FIFTH CIRCUIT RULE 39

39.1 Taxable Rates. *The cost of reproducing necessary copies of the brief, appendices, or record excerpts shall be taxed at a rate not higher than \$0.15 per page, including cover, index, and internal pages, for any for of reproduction costs. The cost of the binding required by 5TH CIR. R. 32.2.3 that mandates that briefs must lie reasonably flat when open shall be a taxable cost but not limited to the foregoing rate. This rate is intended to approximate the current cost of the most economical acceptable method of reproduction generally available; and the clerk shall, at reasonable intervals, examine and review it to reflect current rates. Taxable costs will be authorized for up to 15 copies for a brief and 10 copies of an appendix or record excerpts, unless the clerk gives advance approval for additional copies.*

39.2 Nonrecovery of Mailing and Commercial Delivery Service Costs. *Mailing and commercial delivery fees incurred in transmitting briefs are not recoverable as taxable costs.*

39.3 Time for Filing Bills of Costs. *The clerk must receive bills of costs and any objections within the times set forth in FED. R. APP. P. 39(d). See 5TH CIR. R. 26.1.*

FED. R. APP. P. 39. COSTS

(a) Against Whom Assessed. The following rules apply unless the law provides or the court orders otherwise;

- (1) if an appeal is dismissed, costs are taxed against the appellant, unless the parties agree otherwise;
- (2) if a judgment is affirmed, costs are taxed against the appellant;
- (3) if a judgment is reversed, costs are taxed against the appellee;
- (4) if a judgment is affirmed in part, reversed in part, modified, or vacated, costs are taxed only as the court orders.

(b) Costs For and Against the United States. Costs for or against the United States, its agency or officer will be assessed under Rule 39(a) only if authorized by law.

©) **Costs of Copies** Each court of appeals must, by local rule, fix the maximum rate for taxing the cost of producing necessary copies of a brief or appendix, or copies of records authorized by rule 30(f). The rate must not exceed that generally charged for such work in the area where the clerk's office is located and should encourage economical methods of copying.

(d) Bill of costs: Objections; Insertion in Mandate.

- (1) A party who wants costs taxed must – within 14 days after entry of judgment – file with the circuit clerk, with proof of service, an itemized and verified bill of costs.
- (2) Objections must be filed within 14 days after service of the bill of costs, unless the court extends the time.
- (3) The clerk must prepare and certify an itemized statement of costs for insertion in the mandate, but issuance of the mandate must not be delayed for taxing costs. If the mandate issues before costs are finally determined, the district clerk must – upon the circuit clerk's request – add the statement of costs, or any amendment of it, to the mandate.
- (e) **Costs of Appeal Taxable in the District Court.** The following costs on appeal are taxable in the district court for the benefit of the party entitled to costs under this rule:
 - (1) the preparation and transmission of the record;
 - (2) the reporter's transcript, if needed to determine the appeal;
 - (3) premiums paid for a supersedeas bond or other bond to preserve rights pending appeal; and
 - (4) the fee for filing the notice of appeal.

United States Court of Appeals

FIFTH CIRCUIT
OFFICE OF THE CLERK

LYLE W. CAYCE
CLERK

TEL. 504-310-7700
600 S. MAESTRI PLACE
NEW ORLEANS, LA 70130

September 20, 2016

MEMORANDUM TO COUNSEL OR PARTIES LISTED BELOW

Regarding: Fifth Circuit Statement on Petitions for Rehearing
or Rehearing En Banc

No. 15-50759 Defense Distributed, et al v. U.S. Dept. of
State, et al
USDC No. 1:15-CV-372

Enclosed is a copy of the court's decision. The court has entered judgment under FED R. APP. P. 36. (However, the opinion may yet contain typographical or printing errors which are subject to correction.)

FED R. APP. P. 39 through 41, and 5TH CIR. R.s 35, 39, and 41 govern costs, rehearings, and mandates. **5TH CIR. R.s 35 and 40 require you to attach to your petition for panel rehearing or rehearing en banc an unmarked copy of the court's opinion or order.** Please read carefully the Internal Operating Procedures (IOP's) following FED R. APP. P. 40 and 5TH CIR. R. 35 for a discussion of when a rehearing may be appropriate, the legal standards applied and sanctions which may be imposed if you make a nonmeritorious petition for rehearing en banc.

Direct Criminal Appeals. 5TH CIR. R. 41 provides that a motion for a stay of mandate under FED R. APP. P. 41 will not be granted simply upon request. The petition must set forth good cause for a stay or clearly demonstrate that a substantial question will be presented to the Supreme Court. Otherwise, this court may deny the motion and issue the mandate immediately.

Pro Se Cases. If you were unsuccessful in the district court and/or on appeal, and are considering filing a petition for certiorari in the United States Supreme Court, you do not need to file a motion for stay of mandate under FED R. APP. P. 41. The issuance of the mandate does not affect the time, or your right, to file with the Supreme Court.

Court Appointed Counsel. Court appointed counsel is responsible for filing petition(s) for rehearing(s) (panel and/or en banc) and writ(s) of certiorari to the U.S. Supreme Court, unless relieved of your obligation by court order. If it is your intention to file a motion to withdraw as counsel, you should notify your client promptly, **and advise them of the time limits for filing for rehearing and certiorari.** Additionally, you MUST confirm that this information was given to your client, within the body of your motion to withdraw as counsel.

The judgment entered provides that plaintiffs-appellants pay to defendants-appellees the costs on appeal.

Sincerely,

LYLE W. CAYCE, Clerk

Jamei R. Schaeffer

By: _____

Jamei R. Schaeffer, Deputy Clerk

Enclosure(s)

Mr. Joshua Michael Blackman
Mr. Bruce D. Brown
Mr. Matthew Goldstein
Mr. Alan Gura
Mr. David T. Hardy
Mr. Robert E. Henneke
Mr. John Devereux Kimball
Mr. Martin Simon Krezalek
Mr. William Bryan Mateja
Mr. Raffi Melkonian
Mr. Randal John Meyer
Mr. David Scott Morris
Mr. Leif A. Olson
Mr. Michael S. Raab
Mr. Ilya Shapiro
Mr. Joel Stonedale
Mr. Daniel Bentele Hahs Tenny
Mr. Kit Walsh

United States Senate

WASHINGTON, DC 20510

DEC 01 2016

November 21, 2016

The Honorable John Kerry
 Secretary of State
 U.S. Department of State
 2201 C St. NW
 Washington, DC 20520

RECEIVED
 2016 DEC -1 P 1:50
 LEGISLATIVE AFFAIRS

Dear Secretary Kerry:

We understand that Categories I, II and III of the International Trafficking in Arms Regulations (ITAR), which control combat rifles, shotguns, ammunition and associated equipment and parts, are the last categories to be reviewed under the President's Export Control Reform (ECRI). We also understand that the Department of State is under some pressure to complete the review of these categories and submit the required congressional notification to Congress of the results, including what items are to be removed from these categories and transferred to the Department of Commerce's control list, before the end of the calendar year.

We fully support the ECRI efforts to date. These changes have rationalized and streamlined a cumbersome and opaque U.S. Munitions List (USML) in ways that make it more useful for American exporters to understand and to make non-militarily-sensitive exports easier and more competitive internationally.


However, we are concerned that any changes made to Categories I, II and III be cautious and incremental. As you are aware, combat firearms and ammunition are uniquely lethal; they are easily spread and easily modified, and are the primary means of injury and destruction in civil and military conflicts throughout the world. As such, they should be subject to more, not less, rigorous export controls and oversight. Congress amended the Arms Export Control Act in 2002 to ensure that these arms would receive closer scrutiny than other weapon systems, by setting a lower reporting threshold (from \$14 Million to \$1 Million) specifically for combat rifles on the USML. Moving these rifles off the USML to the Department of Commerce would circumvent Congress's 2002 action, and eliminate Congressional oversight and review of these weapons.

At the very least, combat rifles commonly known as "sniper rifles" should not be removed from the USML; nor should rifles of any type that are U.S. military-standard 5.56 (and especially .50 caliber). Automatic firearms should clearly not be removed, nor should semi-automatic "assault-type" rifles. Ammunition for all these types of firearms should clearly not be removed from USML controls, nor should associated manufacturing equipment, technology or knowledge.

Sincerely,


 BENJAMIN L. CARDIN
 United States Senator


 DIANNE FEINSTEIN
 United States Senator


 PATRICK J. LEAHY
 United States Senator



United States Department of State

Washington, D.C. 20520

JAN 26 2017

The Honorable
Benjamin L. Cardin
United States Senate
Washington, DC 20510

Dear Senator Cardin:

Thank you for your letter dated November 21, 2016 outlining your collective concerns regarding possible changes to Categories I, II, and III of the United States Munitions List (USML), which control combat firearms and rifles, shotguns, ammunition and associated parts and components; guns and armament; and ammunition and ordnance, respectively.

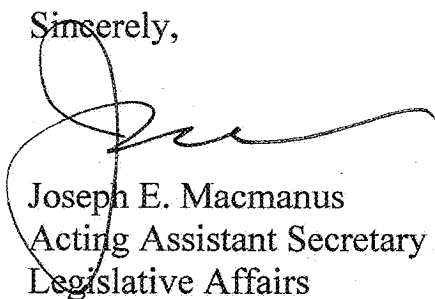
Categories I, II, and III have remained on hold as the Department of State completed its initial review of the other 18 categories of the USML, the last associated rulemaking of which was published on January 10, 2017 (regarding Category XV, Spacecraft and Related Articles). While no decisions have yet been made on the next steps for Categories I-III, the Department of State recognizes the sensitivities concerning firearms and notes your specific concerns. In recognition of these sensitivities, it should be noted that if a decision is made to move certain firearms to the jurisdiction of the Department of Commerce, the Secretary of Commerce is required by Executive Order 13637 to establish appropriate procedures for notifying Congress.

Finally, please note that any proposed changes to these categories will be subject to notice and public comment through the rulemaking process, and as the Department of State has done throughout the Export Control Reform initiative, we will share any draft proposed rules with Congress. At the end of any proposed and final rulemaking process, should the Department seek to remove any defense articles or defense services from the USML, we will notify Congress in accordance with section 38(f) of the Arms Export Control Act. We stand by to provide additional information as requested.

- 2 -

We hope this information is useful. Please do not hesitate to let us know if we can be of further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Macmanus', is written over the typed name and title.

Joseph E. Macmanus
Acting Assistant Secretary
Legislative Affairs



United States Department of State

Washington, D.C. 20520

JAN 26 2017

The Honorable
Patrick J. Leahy
United States Senate
Washington, DC 20510

Dear Senator Leahy:

Thank you for your letter dated November 21, 2016 outlining your collective concerns regarding possible changes to Categories I, II, and III of the United States Munitions List (USML), which control combat firearms and rifles, shotguns, ammunition and associated parts and components; guns and armament; and ammunition and ordnance, respectively.

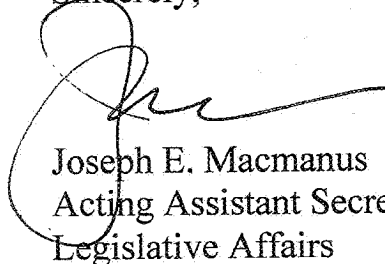
Categories I, II, and III have remained on hold as the Department of State completed its initial review of the other 18 categories of the USML, the last associated rulemaking of which was published on January 10, 2017 (regarding Category XV, Spacecraft and Related Articles). While no decisions have yet been made on the next steps for Categories I-III, the Department of State recognizes the sensitivities concerning firearms and notes your specific concerns. In recognition of these sensitivities, it should be noted that if a decision is made to move certain firearms to the jurisdiction of the Department of Commerce, the Secretary of Commerce is required by Executive Order 13637 to establish appropriate procedures for notifying Congress.

Finally, please note that any proposed changes to these categories will be subject to notice and public comment through the rulemaking process, and as the Department of State has done throughout the Export Control Reform initiative, we will share any draft proposed rules with Congress. At the end of any proposed and final rulemaking process, should the Department seek to remove any defense articles or defense services from the USML, we will notify Congress in accordance with section 38(f) of the Arms Export Control Act. We stand by to provide additional information as requested.

- 2 -

We hope this information is useful. Please do not hesitate to let us know if we can be of further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Macmanus', is written over the printed name and title.

Joseph E. Macmanus
Acting Assistant Secretary
Legislative Affairs



United States Department of State

Washington, D.C. 20520

JAN 26 2017

The Honorable
Dianne Feinstein
United States Senate
Washington, DC 20510

Dear Senator Feinstein:

Thank you for your letter dated November 21, 2016 outlining your collective concerns regarding possible changes to Categories I, II, and III of the United States Munitions List (USML), which control combat firearms and rifles, shotguns, ammunition and associated parts and components; guns and armament; and ammunition and ordnance, respectively.

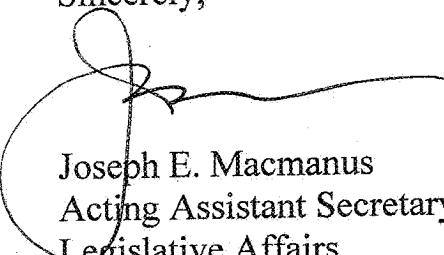
Categories I, II, and III have remained on hold as the Department of State completed its initial review of the other 18 categories of the USML, the last associated rulemaking of which was published on January 10, 2017 (regarding Category XV, Spacecraft and Related Articles). While no decisions have yet been made on the next steps for Categories I-III, the Department of State recognizes the sensitivities concerning firearms and notes your specific concerns. In recognition of these sensitivities, it should be noted that if a decision is made to move certain firearms to the jurisdiction of the Department of Commerce, the Secretary of Commerce is required by Executive Order 13637 to establish appropriate procedures for notifying Congress.

Finally, please note that any proposed changes to these categories will be subject to notice and public comment through the rulemaking process, and as the Department of State has done throughout the Export Control Reform initiative, we will share any draft proposed rules with Congress. At the end of any proposed and final rulemaking process, should the Department seek to remove any defense articles or defense services from the USML, we will notify Congress in accordance with section 38(f) of the Arms Export Control Act. We stand by to provide additional information as requested.

- 2 -

We hope this information is useful. Please do not hesitate to let us know if we can be of further assistance.

Sincerely,



Joseph E. Macmanus
Acting Assistant Secretary
Legislative Affairs

16-315-cv
Stagg P.C. v. U.S. Dep't of State

**UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT**

SUMMARY ORDER

RULINGS BY SUMMARY ORDER DO NOT HAVE PRECEDENTIAL EFFECT. CITATION TO A SUMMARY ORDER FILED ON OR AFTER JANUARY 1, 2007, IS PERMITTED AND IS GOVERNED BY FEDERAL RULE OF APPELLATE PROCEDURE 32.1 AND THIS COURT'S LOCAL RULE 32.1.1. WHEN CITING A SUMMARY ORDER IN A DOCUMENT FILED WITH THIS COURT, A PARTY MUST CITE EITHER THE FEDERAL APPENDIX OR AN ELECTRONIC DATABASE (WITH THE NOTATION "SUMMARY ORDER"). A PARTY CITING A SUMMARY ORDER MUST SERVE A COPY OF IT ON ANY PARTY NOT REPRESENTED BY COUNSEL.

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 16th day of December, two thousand sixteen.

PRESENT: GUIDO CALABRESI,
REENA RAGGI,
GERARD E. LYNCH,
Circuit Judges.

STAGG P.C.,
Plaintiff-Appellant,

v.

No. 16-315-cv

UNITED STATES DEPARTMENT OF STATE,
DIRECTORATE OF DEFENSE TRADE CONTROLS,
JOHN KERRY, in his official capacity only as Secretary
of State,

Defendants-Appellees.

APPEARING FOR APPELLANT: LAWRENCE D. ROSENBERG (Christopher
B. Stagg, Stagg P.C., New York, New York, *on the brief*), Jones Day, Washington D.C.

APPEARING FOR APPELLEE: DOMINIKA TARCZYNSKA, Assistant United
States Attorney (Benjamin H. Torrance,
Assistant United States Attorney, *on the brief*),
for Preet Bharara, United States Attorney for

the Southern District of New York, New York,
New York.

Appeal from an order of the United States District Court for the Southern District of New York (Shira A. Scheindlin, *Judge*) denying a preliminary injunction.

UPON DUE CONSIDERATION, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED that the order entered on January 26, 2016, is AFFIRMED.

Plaintiff Stagg P.C. appeals from the denial of its motion for a preliminary injunction against the government’s imposition of the registration and licensing mandates of the Arms Export Control Act (“AECA”), 22 U.S.C. § 2778, and the International Traffic in Arms Regulations (“ITAR”), 22 C.F.R. §§ 120–130, which regulate the dissemination of information related to items enumerated on the United States Munitions List, *see* 22 C.F.R. § 121. Specifically, the requested injunction would have broadly enjoined the government from “enforcing *any* licensing or other approval requirements for putting privately generated unclassified information *into* the public domain.” J.A. 8 (emphases added). Our jurisdiction to review the denial order is established by 28 U.S.C. § 1292(a)(1).

Stagg alleges that the challenged licensing system is (1) an unconstitutional prior restraint under the First Amendment and (2) impermissibly vague under the Fifth Amendment. While defending the district court’s injunction denial, the government challenges its ruling that Stagg has standing to maintain this action. We review (1) a determination as to standing *de novo*; and (2) the denial of a preliminary injunction for abuse of discretion, which we will identify only where a decision rests on an error of law or clearly erroneous finding of fact. *See Nicosia v. Amazon, Inc.*, 834 F.3d 220, 238 (2d

Cir. 2016). In so doing, we assume the parties' familiarity with the facts and record of prior proceedings, which we reference only as necessary to explain our decision to affirm substantially for the reasons stated by the district court. *See Stagg P.C. v. U.S. Dep't of State*, 158 F. Supp. 3d 203 (S.D.N.Y. 2016).

1. Standing

The district court determined that, "under the lenient standing requirements in prior restraint cases," Stagg has standing to pursue this action because it "alleges that it possesses certain technical data . . . that it wants to aggregate into a set of materials for presentation to an audience," which "requires prior approval from the DDTC under the AECA and the ITAR." *Id.* at 209. We agree.

In stating that (1) it presently seeks to disseminate information already in its possession subject to ITAR's challenged licensing requirement and (2) it has already refrained from doing so for fear of being sanctioned, Stagg has alleged the "real or immediate threat" of future injury necessary for standing. *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983); *see Meese v. Keene*, 481 U.S. 465, 473 (1987) (determining that affidavit stating that challenged law had deterred plaintiff from exhibiting films established standing). Moreover, a licensing regime is subject to facial challenge as a prior restraint when it "allegedly vests unbridled discretion in a government official over whether to permit or deny" publication of speech, even "without the necessity of [plaintiff's] first applying for, and being denied, a license." *City of Lakewood v. Plain*

Dealer Publ'g Co., 486 U.S. 750, 755–56 (1988). Accordingly, the district court correctly rejected the government’s standing challenge to this action.¹

2. Preliminary Injunction

A plaintiff seeking a preliminary injunction must establish that (1) he is likely to succeed on the merits, (2) he is likely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities tips in his favor, and (4) an injunction is in the public interest. *See Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008).

The district court determined that the third and fourth factors required denial of the preliminary injunction here to avoid “very serious adverse impacts” to national security. *Stagg P.C. v. U.S. Dep’t of State*, 158 F. Supp. 3d at 210. We agree.

The content of the speech in question is “technical data,” which ITAR defines as “[i]nformation . . . required for [*inter alia*] the design, development, [and] production . . . of defense articles.” 22 C.F.R. § 120.10(a). Because Stagg (1) has elected not to identify, even to the district court, the specific content of the material it seeks to publish, *see Stagg P.C. v. U.S. Dep’t of State*, 158 F. Supp. 3d at 208; and (2) has requested a broad injunction against “any licensing or other approval requirements for putting

¹ We note that many of Stagg’s arguments on appeal could be read as attacking not the existing regulatory scheme, but either a proposed regulation that was never adopted, or a prior regulation that Stagg claims was once in force but has since been repealed. Constitutional questions about regulations that no longer exist or that have been under consideration do not present cases or controversies within a court’s Article III jurisdiction. *See Nat’l Org. for Marriage, Inc. v. Walsh*, 714 F.3d 682, 687 (2d Cir. 2013) (“A claim is not ripe if it depends upon contingent future events that may not occur as anticipated, or indeed may not occur at all.” (internal quotation marks omitted)). Here, however, the government unambiguously confirmed at oral argument that Stagg correctly characterizes the government’s interpretation of the existing regulatory scheme (as noted below). Thus, we agree that Stagg has standing to challenge that scheme as the government construes it.

privately generated unclassified information *into* the public domain,” J.A. 8 (emphases added) (an injunction which we note would apply also to material that is not presently publicly available), the district court appropriately “assume[d] the worst case scenario,” *i.e.*, that the material at issue might communicate, for example, “technical data for delivery systems for weapons of mass destruction,” or for “chemical and biological agents,” or “plans for 3D-printable plastic firearms,” *Stagg P.C. v. U.S. Dep’t of State*, 158 F. Supp. 3d at 210 n.47 & 210–11.

The national security concerns raised by a preliminary injunction that barred the government from licensing, and thereby controlling, the dissemination of such sensitive information are obvious and significant. We note that the government does not merely invoke national security as “a broad, vague generality” of the sort that cannot “abrogate the fundamental law embodied in the First Amendment.” *New York Times Co. v. United States*, 403 U.S. 713, 719 (1971) (Black, J., concurring). Rather, it has set forth specific concerns relating to the export of “technical data” as defined in ITAR. As a State Department official explained in a sworn affidavit, a preliminary injunction would “cause significant harm to the national security and foreign policy interest of the United States,” due to the potential for “[u]ncontrolled disclosure of technical data on the development, production, or deployment of weapons of mass destruction” or “the potential release of technical data for delivery systems of” such weapons to “someone set on creating mass, indiscriminate, civilian casualties” or a “foreign adversary.” J.A. 95. Indeed, “[a]bsent the inclusion of ‘technical data[]’” within ITAR’s licensing structure, the statutory “limits on arms transfers would be of negligible practical effect because [they] would leave unregulated the exportation of the technology, know-how, blueprints, and other design

information sufficient for foreign powers to construct, produce, manufacture, maintain, and operate the very same equipment regulated in its physical form by the ITAR.” *Id.* at 90. In matters of national security, which present the most compelling national interest, *see Haig v. Agee*, 453 U.S. 280, 307 (1981); *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 826 (2d Cir. 2015), we accord considerable “deference” to such an “evaluation of the facts by the Executive,” *Holder v. Humanitarian Law Project*, 561 U.S. 1, 33 (2010); *see also Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. at 27. Thus, the government presents a valid case—unrefuted by Stagg—for balancing the equities in their favor and finding that the public interest weighs against this injunction.

Stagg contends that the district court’s reliance solely on national security to deny the preliminary injunction is foreclosed by *New York Times Co. v. United States*, 403 U.S. 713. We are not persuaded. While it could not be said that disclosure of the materials there at issue would “result in direct, immediate, and irreparable damage to our Nation or its people,” *id.* at 730 (Stewart, J., concurring), that is just the conclusion that the district court was entitled to draw here so long as Stagg refuses to disclose to a court the information it wants to shield from ITAR. Further, here we deal with a statutorily authorized regulatory scheme, which implicates legislative as well as executive judgment about the national security interest in controlling information for the production of defense articles on the U.S. Munitions List. *See id.* at 718 (Black, J., concurring).

Having carefully scrutinized the specific national security interests presented by the government, we conclude that its stated interests outweigh Stagg’s claimed harm. The government has articulated specific, concrete damage to national security that could result if the district court entered Stagg’s broad proposed injunction. The specificity of

the government's contentions contrasts sharply with the vagueness of Stagg's allegations and its refusal to provide the district court with sufficient information to assess the plausibility of the government's national security arguments. Thus, the district court did not abuse its discretion when it found that the public interest in maintaining national security weighed against granting a preliminary injunction in this case.

In these circumstances, where the balance-of-equities and public interest factors weigh so heavily against a preliminary injunction, we need not decide whether Stagg is likely to succeed on the merits or to suffer irreparable harm. *See American Civil Liberties Union v. Clapper*, 785 F.3d at 826 (declining to order preliminary injunction in light of national security interests even where success on merits was certain); *see also Defense Distributed v. U.S. Dep't of State*, 838 F.3d 451, 458 (5th Cir. 2016) (affirming denial of preliminary injunction against ITAR on balance-of-equities and public interest factors alone). Accordingly, we identify no abuse of discretion in the district court's denial decision.

But just as Stagg's refusal to disclose—even to the district court—the information it seeks to publish, and whether that information is already publicly available, makes it appropriate to deny the broad preliminary injunction sought, we note concern with the government's representations at oral argument. Specifically, government counsel argued that ITAR applies to *republication* of information already in the public domain. While a June 3, 2015 proposed rule would add a subsection to the definition of “public domain” making clear that “[t]echnical data . . . is not in the public domain if it has been made available to the public [initially] without authorization,” 80 Fed. Reg. 31,525, 31,535, and would proscribe the “mak[ing] available to the public [of] technical data . . .

if [a party] has knowledge that the technical data . . . was [first] made publicly available without an authorization in § 120.11(b),” *id.* at 31,538, it is unclear where in the *current* ITAR such a prohibition can be located. Indeed, government counsel was unable to direct us to a provision that qualifies 22 C.F.R. § 120.10(b), which presently exempts from the definition of technical data, subject to ITAR, *inter alia*, “information in the public domain as defined in § 120.11.” We do not pursue the point further here or predict how it might be decided on full briefing. We state only that, while we affirm the order denying the broad injunction sought by Stagg, we do so without prejudice to the pursuit of narrower relief in the district court.²

3. Conclusion

We have considered Stagg’s remaining arguments and conclude that they are without merit. Accordingly, we AFFIRM without prejudice the order denying preliminary injunctive relief.

FOR THE COURT:
Catherine O’Hagan Wolfe, Clerk of Court


² Insofar as comments in the district court’s opinion are skeptical of a narrower injunction, we do not understand them to reflect any ruling, particularly as no narrower relief or supportive briefing was then before the court.


2017-2018

A stated goal of ECR is, "Improving the long-term health and competitiveness of the U.S. industrial base, which includes maintaining and expanding jobs." To maximize the positive economic impacts of ECR, the relevant agencies must complete their work on the remaining USML categories. Our states are home to world-class firearm and ammunition manufacturers. With streamlined regulations, these important businesses will be able to access new markets, create new jobs, and hire hard-working Americans.


We will continue to be vocal supporters of completing ECR to ensure American businesses are able to be competitive in the export market while also bolstering the security of the United States. We stand ready to assist you in completing this process.


Sincerely,

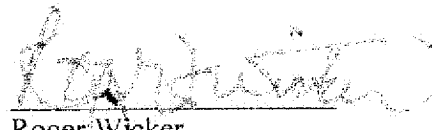

Jon Fester
United States Senator


John Boozman
United States Senator



Heidi Heitkamp
United States Senator



Steve Daines
United States Senator


Amy Klobuchar
United States Senator

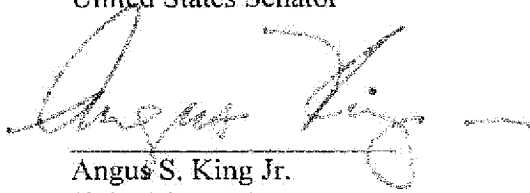

Roger Wicker
United States Senator

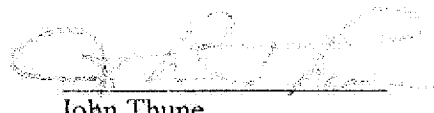

Joe Donnelly
United States Senator

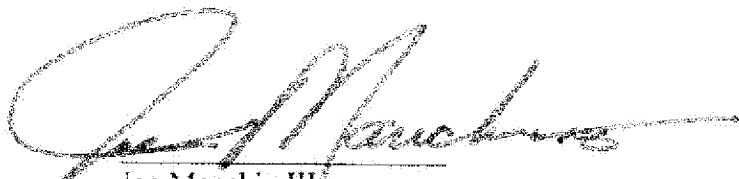

Jerry Moran
United States Senator


Martin Heinrich
United States Senator


John Cornyn
United States Senator


Angus S. King Jr.
United States Senator



John Thune
United States Senator



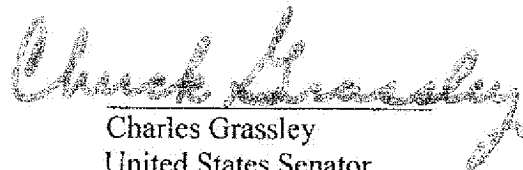
Joe Manchin III
United States Senator




Mike Crapo
United States Senator



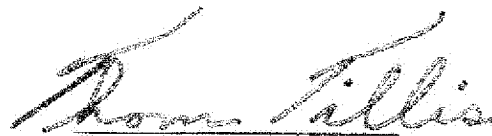
Jim Risch
United States Senator



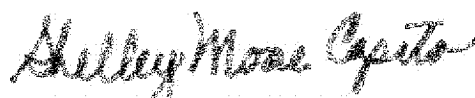
Charles Grassley
United States Senator



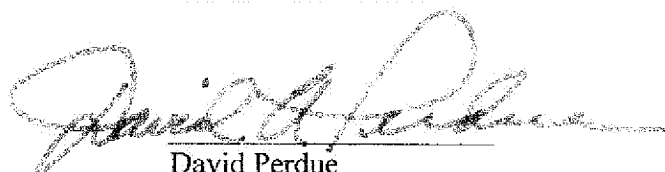
Jim Inhofe
United States Senator



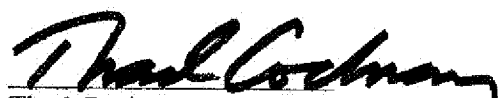
Thom Tillis
United States Senator



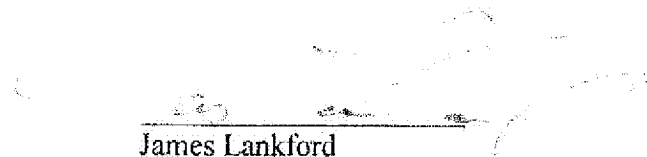
Shelley Moore Capito
United States Senator



David Perdue
United States Senator



Thad Cochran
United States Senator



James Lankford
United States Senator



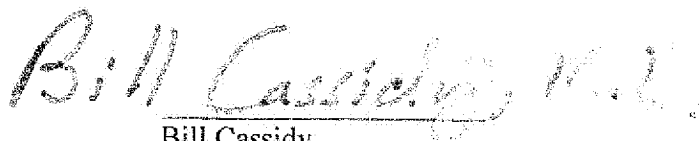
Susan Collins
United States Senator



Pat Roberts
United States Senator



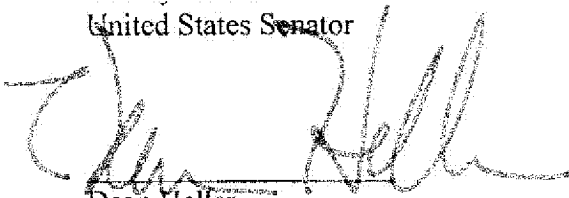
M. Michael Rounds
United States Senator



Bill Cassidy
United States Senator



Johnny Isakson
United States Senator



Dean Heller
United States Senator



Ted Cruz
United States Senator



United States Department of State

Washington, D.C. 20520

MAY 23 2017

The Honorable
Jon Tester
United States Senate
Washington, DC 20510

Dear Senator Tester:

Thank you for your letter of May 1 expressing continued support for the Export Control Reform Initiative.

The Department of State and the Department of Commerce have benefitted from the broad bipartisan support of the Congress for our multi-year efforts to modernize the U.S. export control system. With Congress' support, we have made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations and the Export Administration Regulations. We also have revised 18 of the 21 Categories on the United States Munitions List controlled by the Department of State and made corresponding revisions to the Commerce Control List. We are finalizing the three remaining categories of controls, with the goal of obtaining guidance to publish them for public comment as we did for the other 18 categories. This process was requested by industry, including the firearms and ammunition industry, to ensure the rules are clear and implementable.

We hope you find this information helpful and appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Joe Macmanus", with a long horizontal line extending to the right.

Joseph E. Macmanus
Bureau of Legislative Affairs

Congress of the United States
Washington, DC 20515

May 3, 2017

The Honorable Rex W. Tillerson
Secretary of State
2201 C Street NW
Washington, D.C. 20520

The Honorable Wilbur L. Ross
Secretary of Commerce
1401 Constitution Avenue NW
Washington, D.C. 20230

Dear Secretary Tillerson and Secretary Ross:

We write to respectfully urge you to complete the Export Control Reform (ECR) Initiative, which was launched nearly eight years ago and has bipartisan support in Congress.

The very basis of this effort is the common sense notion that products intended only for military use should be subject to the highest standards of security and oversight, while regulation of products with general commercial applications should not unnecessarily hinder American business and innovation.

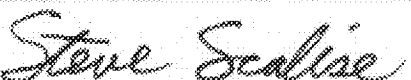
As part of the initiative, regulatory responsibility for dual use items on the United States Munitions List (USML) has been transferred from the State Department to the Commerce Department. So far, eighteen categories have been transferred. Only three remain, and these remaining categories contain the same sorts of constitutionally-protected firearms and ammunition owned by millions of law-abiding Americans. We understand that draft regulations exist to finish the job in this export reform initiative.


In July 2016, the State Department issued guidance that characterized many traditional gunsmiths as “manufacturers” and required them to register as exporters under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), and pay a \$2,250 annual fee. This is unnecessary and is having serious and negative consequences on the hundreds of thousands of small and medium-sized gunsmiths who operate in our districts, as the vast majority of our constituents engaged in gunsmithing make little to no income from their activities and often do it as a hobby or side business. It makes no sense for them to be required to pay \$2,250 and register under AECA and ITAR. Furthermore, not only does the guidance expand registration to gunsmiths who do not “manufacture” firearms, it also runs counter to the intent of AECA and ITAR, which are meant to control the production and exportation of highly sensitive military materiel, not the domestic repair or maintenance of a legal, common, and constitutionally-protected product.

Completion of the Export Control Reform initiative would resolve the problems raised by the July 2016 guidance. It would also enhance our national security and better protect America's most sensitive defense technologies, while improving U.S. competitiveness by reducing unnecessary restrictions on exports of less sensitive commercial items.


Thank you for your consideration of this important issue and we urge you to publish the proposed rules to move the remaining three categories on the USML to Commerce.


Sincerely,

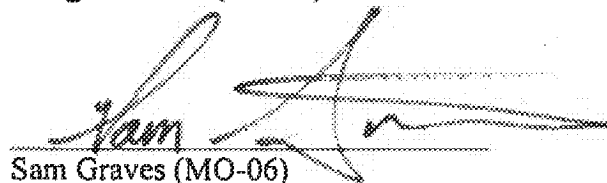

Steve Scalise (LA-01)

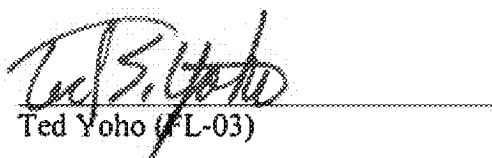

Michael T. McCaul (TX-10)

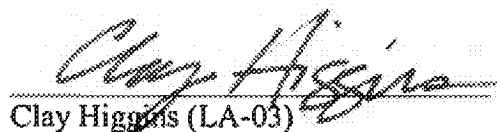

Chris Stewart (UT-02)

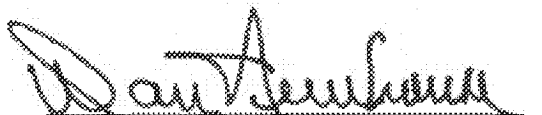

Doug Lamborn (CO-05)

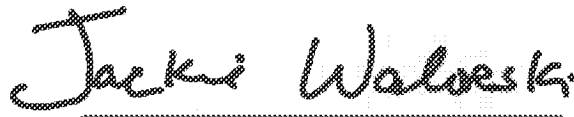

Bradley Byrne (AL-01)

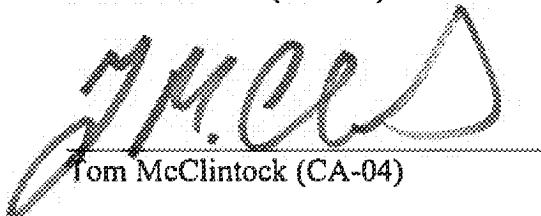

Sam Graves (MO-06)



Ted Yoho (FL-03)



Clay Higgins (LA-03)



Dan Newhouse (WA-04)


Jackie Walorski (IN-02)


Tom McClintock (CA-04)


Vicki Hartzler (MO-04)

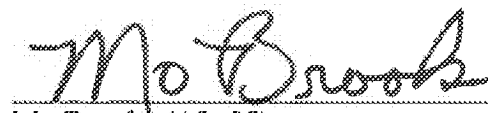

Steve Pearce (NM-02)

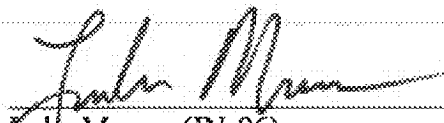

Brian Babin (TX-36)

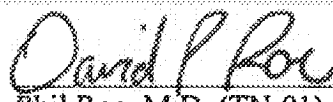

Chuck Fleischmann (TN-03)

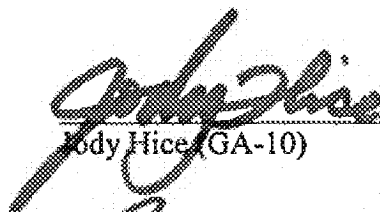

Roger Marshall (KS-01)

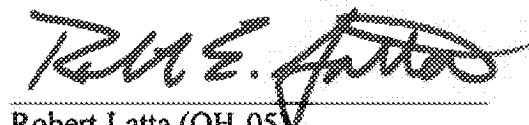

Doug Collins (GA-09)

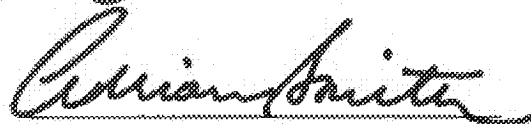

Mo Brooks (AL-05)

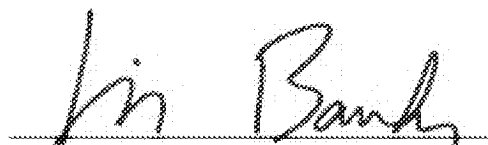

Luke Messer (IN-06)

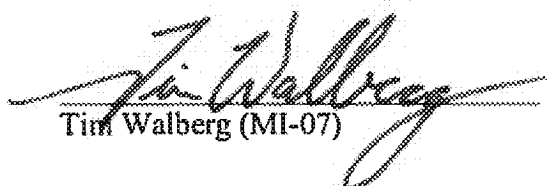

Phil Roe, M.D. (TN-01)

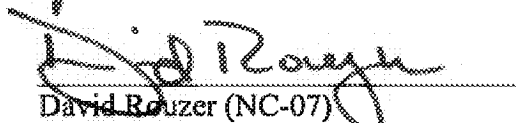

Jody Hice (GA-10)

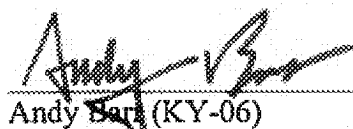

Robert Latta (OH-05)



Adrian Smith (NE-03)

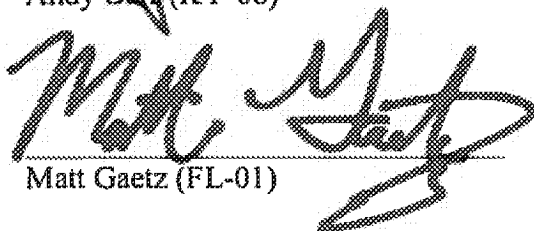

Jim Banks (IN-03)

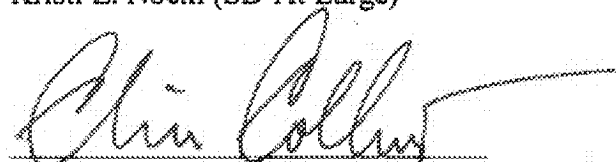

Tim Walberg (MI-07)

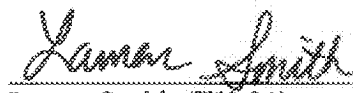

David Rouzer (NC-07)

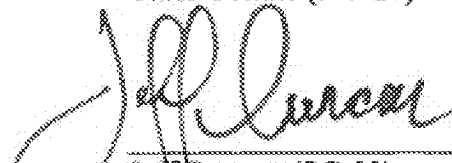

Andy Barr (KY-06)


Kristi L. Noem (SD-At Large)

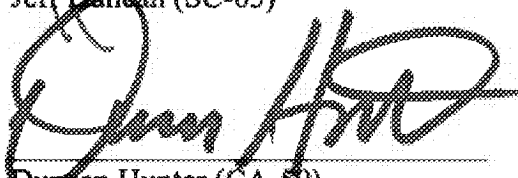

Matt Gaetz (FL-01)



Chris Collins (NY-27)

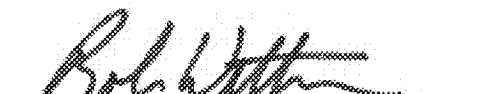

Lamar Smith (TX-21)

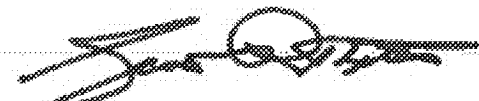

Jeff Duncan (SC-03)

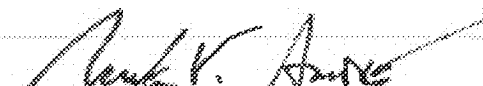

Tom Marino (PA-10)

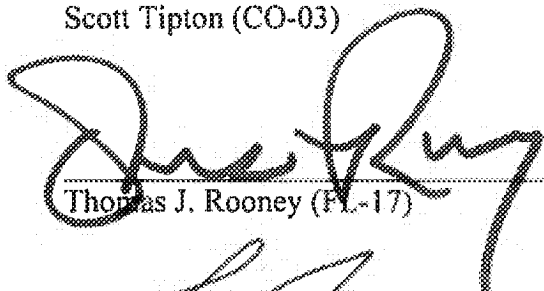

Duncan Hunter (CA-50)


Collin Peterson (MN-07)

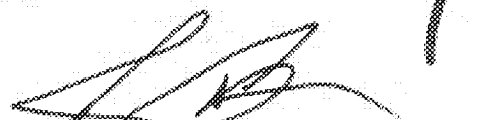

Rob Wittman (VA-01)

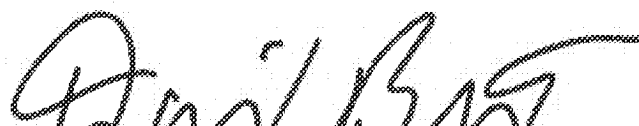

Scott Tipton (CO-03)

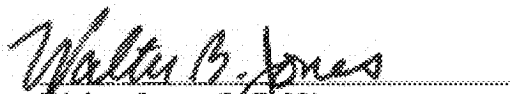

Mark E. Amodei (NV-02)

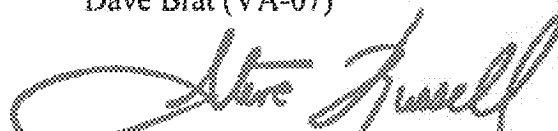

Thomas J. Rooney (FL-17)


Brian Fitzpatrick (PA-08)



Ralph L. Abraham, M.D. (LA-05)


Dave Brat (VA-07)


Walter Jones (NC-03)

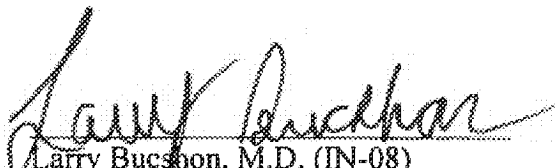

Steve Russell (OK-05)


Richard Hudson (NC-08)

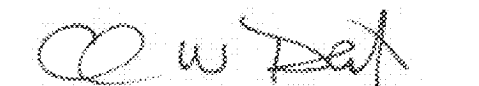

Trent Franks (AZ-08)


Steve Chabot (OH-01)

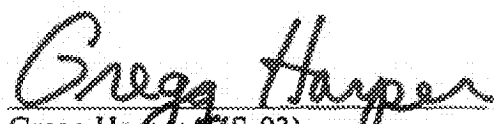

Marsha Blackburn (TN-07)

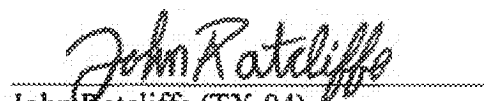

Larry Bucshon, M.D. (IN-08)



Patrick J. Tiberi (OH-12)

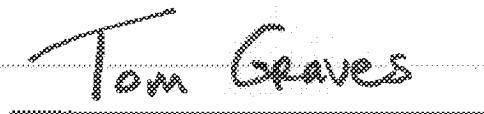

Charles W. Dent (PA-15)



David G. Valadao (CA-21)

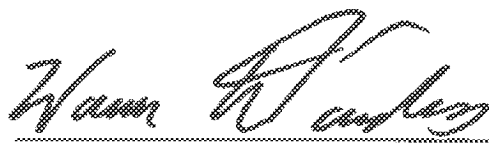

Gregg Harper (MS-03)

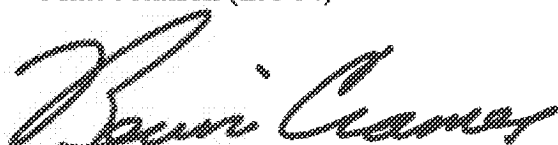

John Ratcliffe (TX-04)


James Comer (KY-01)

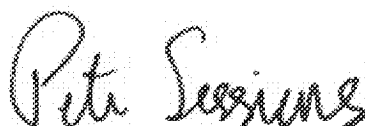

Tom Graves (GA-14)


Mike Johnson (LA-04)

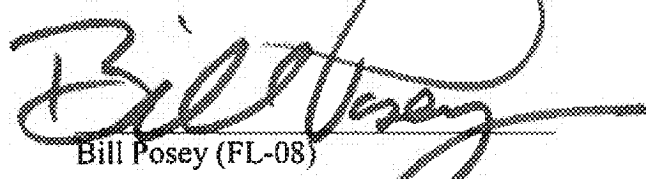

Warren Davidson (OH-08)


Kevin Cramer (ND-At Large)

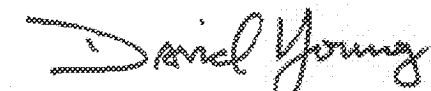

George Holding (NC-02)



Pete Sessions (TX-32)



Glenn "GT" Thompson (PA-05)


Bill Posey (FL-08)

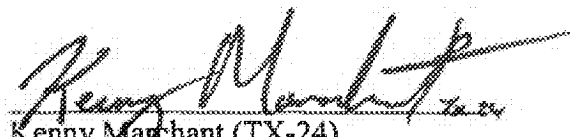

Francis Rooney (FL-19)


David Young (IA-03)

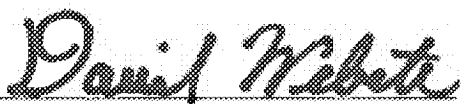

Randy Weber (TX-14)


John Moolenaar (MI-04)

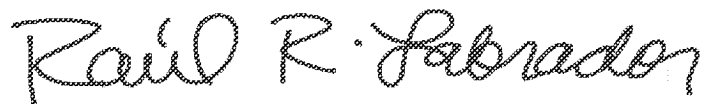

Andy Harris, M.D. (MD-01)


Kenny Marchant (TX-24)


Mark Meadows (NC-11)




Daniel Webster (IL-11)



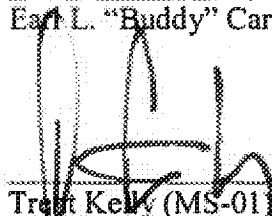
Raúl R. Labrador (ID-01)



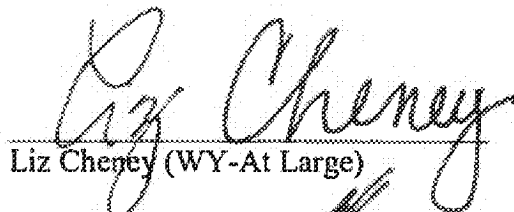
Earl L. "Buddy" Carter (GA-01)



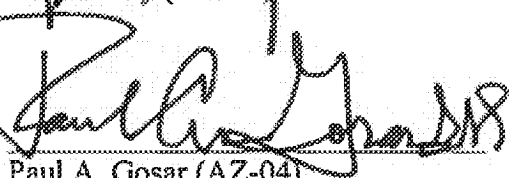
Sam Johnson (TX-03)



Trent Kelly (MS-01)



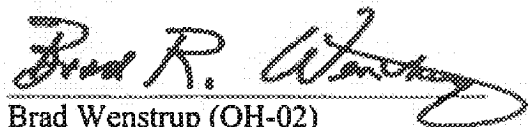
Liz Cheney (WY-At Large)



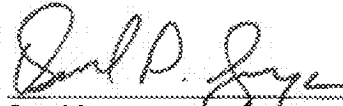
Paul A. Gosar (AZ-04)



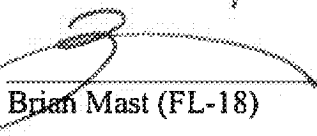
H. Morgan Gohmert (TX-01)



Brad Wenstrup (OH-02)



David Joyce (OH-14)



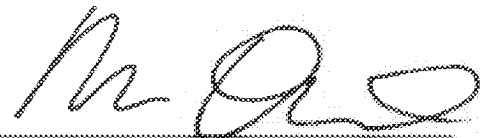
Brian Mast (FL-18)



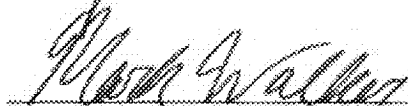
Rick W. Allen (GA-12)



Evan Jenkins (WV-03)



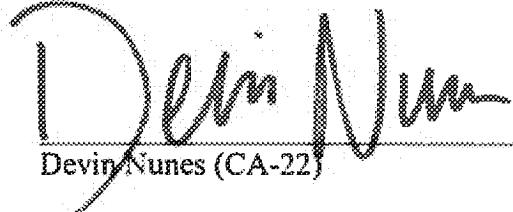
Ron DeSantis (FL-06)



Mark Walker (NC-06)



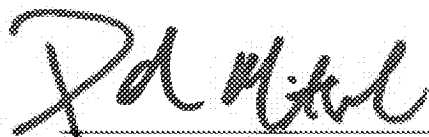
Louie Gohmert (TX-01)



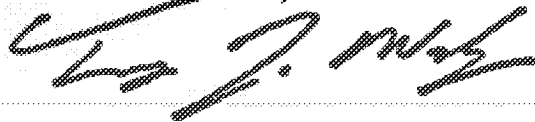
Devin Nunes (CA-22)



Doug LaMalfa (CA-01)



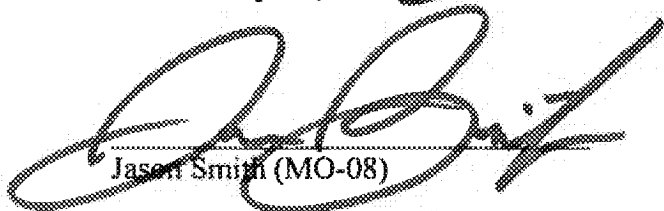
Paul Mitchell (MI-10)



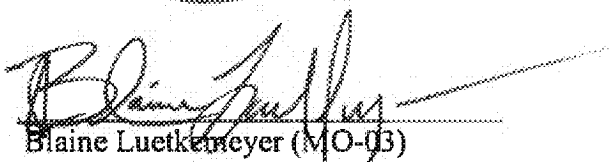
Tim Walz (MN-01)



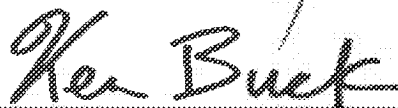
Bruce Poliquin (ME-02)



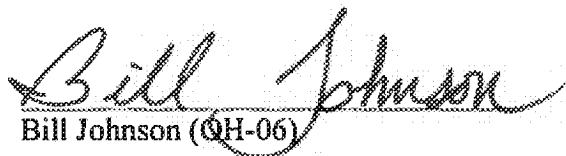
Jason Smith (MO-08)



Blaine Luetkemeyer (MO-03)



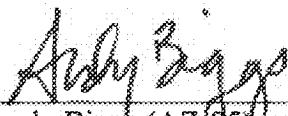
Ken Buck (CO-04)



Bill Johnson (OH-06)



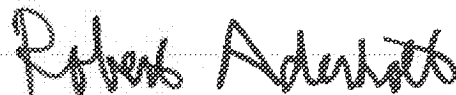
Markwayne Mullin (OK-02)



Andy Biggs (AZ-05)



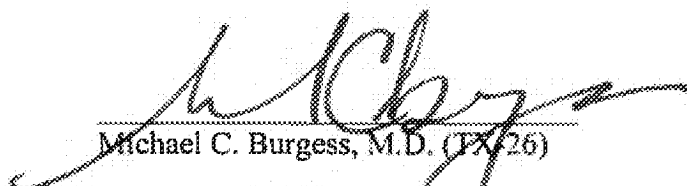
Gus M. Bilirakis (FL-12)



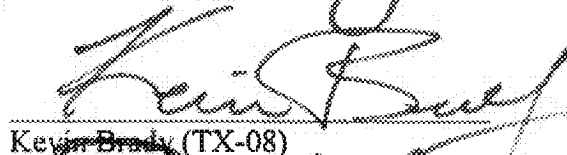
Robert Aderholt (AL-04)



Neal Dunn, M.D. (FL-02)



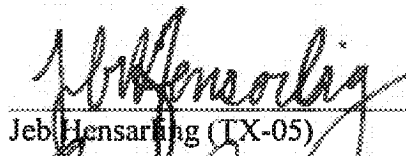
Michael C. Burgess, M.D. (TX-26)



Kevin Brady (TX-08)



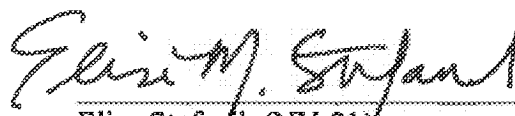
Ron Kind (WI-03)



Jeb Hensarling (TX-05)

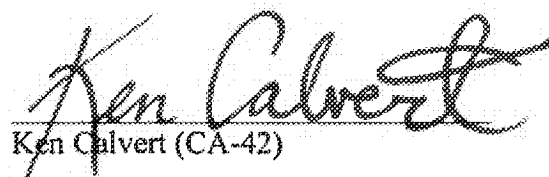


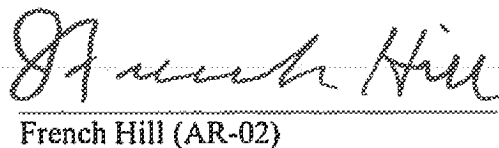
Michael A. Simpson (ID-02)

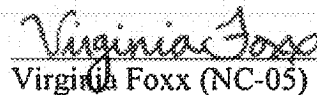


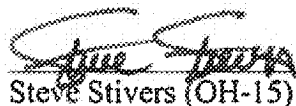
Elise Stefanik (NY-21)


Rob Bishop (UT-01)


Ken Calvert (CA-42)


French Hill (AR-02)

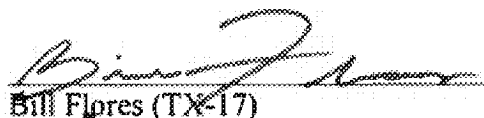

Virginia Foxx (NC-05)

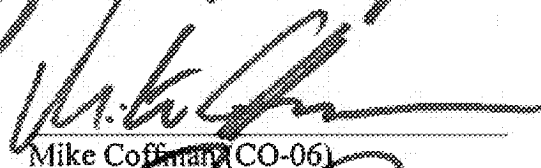

Steve Stivers (OH-15)

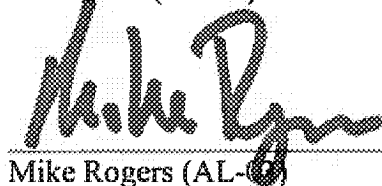

John Culberson (TX-07)

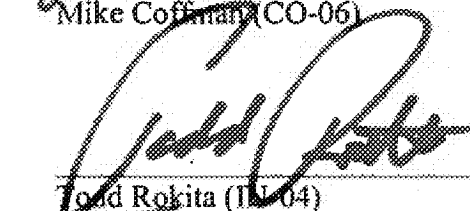

Lloyd Smucker (PA-16)



John Rutherford (FL-04)

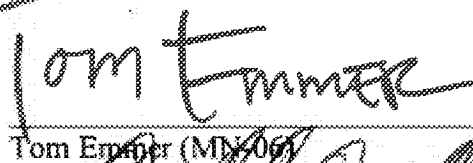

Bill Flores (TX-17)

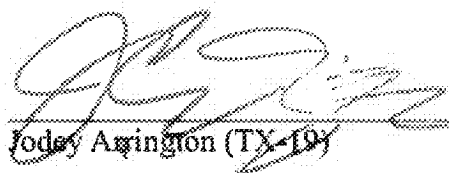

Mike Coffman (CO-06)


Mike Rogers (AL-06)

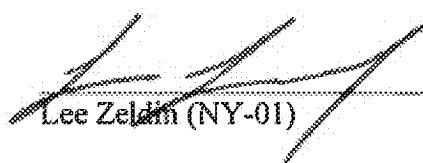

Todd Rokita (IN-04)

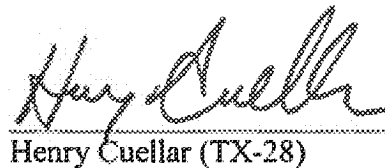

Jeff Dorn (CA-10)


Tom Emmer (MN-06)


Jodey Arrington (TX-19)


Carlos Curbelo (FL-26)


Lee Zeldin (NY-01)

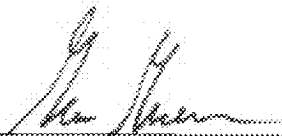

Henry Cuellar (TX-28)



Dennis A. Ross (FL-15)



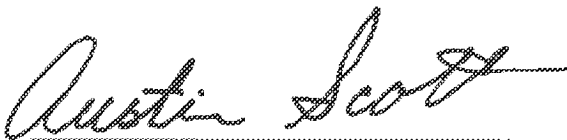
Garret Graves (LA-06)



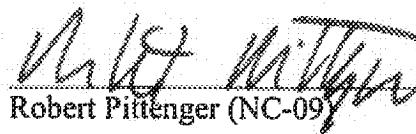
Gene Green (TX-29)



Blake Farenthold (TX-27)



Austin Scott (GA-08)



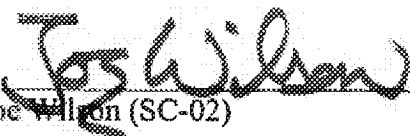
Robert Pittenger (NC-09)



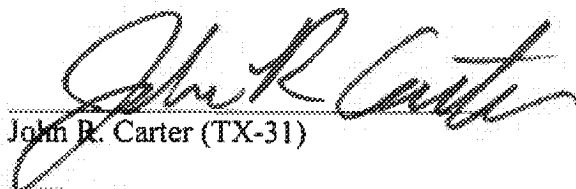
Bruce Westerman (AR-04)



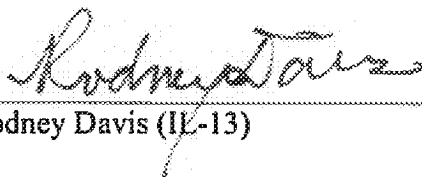
Greg Walden (OR-02)



Joe Wilson (SC-02)



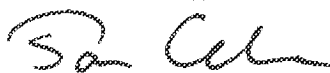
John R. Carter (TX-31)



Rodney Davis (IL-13)



Bob Gibbs (OH-07)



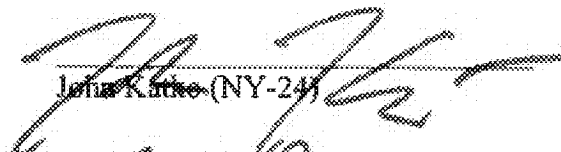
Tom Cole (OK-04)




Bennie G. Thompson (MS-02)



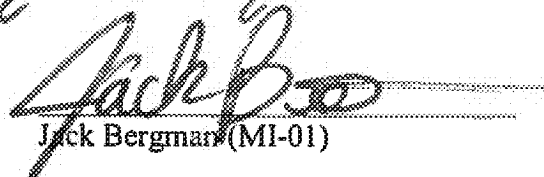
Peter DeFazio (OR-04)



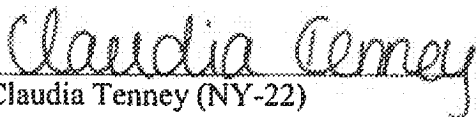
John Katko (NY-24)

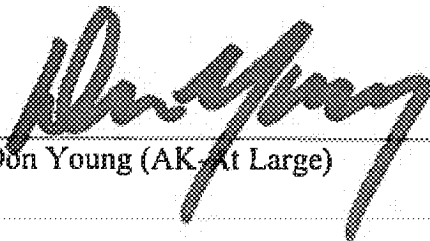


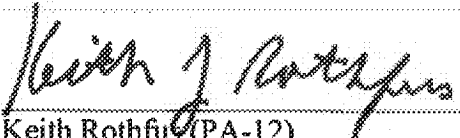
Sean P. Duffy (WI-07)



Jack Bergman (MI-01)


Claudia Tenney (NY-22)


Don Young (AK-At Large)


Keith Rothfus (PA-12)



United States Department of State

Washington, D.C. 20520

MAY 23 2017

The Honorable
Steve Scalise
House of Representatives
Washington, DC 20515

Dear Mr. Scalise:

Thank you for your letter of May 3 expressing continued support for the Export Control Reform Initiative.

The Department of State and the Department of Commerce have benefitted from the broad bipartisan support of the Congress for our multi-year efforts to modernize the U.S. export control system. With Congress' support, we have made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations and the Export Administration Regulations. We also have revised 18 of the 21 Categories on the United States Munitions List controlled by the Department of State and made corresponding revisions to the Commerce Control List. We are finalizing the three remaining categories of controls, with the goal of obtaining guidance to publish them for public comment as we did for the other 18 categories. This process was requested by industry, including the firearms and ammunition industry, to ensure the rules are clear and implementable.

We hope you find this information helpful and appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Joe Macmanus", written over a circular stamp.

Joseph E. Macmanus
Bureau of Legislative Affairs

United States Senate

WASHINGTON, DC 20510

September 15, 2017

The Honorable Rex Tillerson
Secretary of State
U.S. Department of State
2201 C St. NW
Washington, DC 20520

RECEIVED
2017 SEP 26 AM 11:45
LEGISLATIVE AFFAIRS

Dear Secretary Tillerson:

We understand that the Department of State may soon seek to remove lethal small arms, light weapons, and associated equipment and ammunition from Categories I, II, and III of the International Trafficking in Arms Regulations, to be subject instead to the Commerce Control List (CCL) of the Department of Commerce, resulting in less rigorous oversight of related exports.

We support the Export Control Reform Initiative efforts to date. These changes have rationalized and streamlined a cumbersome and opaque U.S. Munitions List (USML) in ways that make it more useful for American exporters to understand and make non-militarily-sensitive exports easier and more competitive internationally.

However, we strongly urge that any changes made to Categories I, II, and III be undertaken with appropriate consideration to the life and death impact such changes will have, and only in consultation with Congress. As you are aware, combat firearms and ammunition are uniquely lethal; they are easily spread and easily modified, and are the primary means of injury, death, and destruction in civil and military conflicts throughout the world. As such, they should be subject to more – not less – rigorous export controls and oversight.

The Arms Export Control Act (AECA) enables congressional review of exports of lethal weapons to ensure that they comport with U.S. foreign policy goals and values. Congress took action in 2002 to ensure that the sale and export of these weapons would receive close scrutiny and oversight, including by amending the AECA to set a lower reporting threshold (from \$14 million to \$1 million) specifically for firearms on the USML. Moving such firearms from the USML to the CCL would be directly contrary to congressional intent, made clear in 2002, effectively eliminating congressional oversight of exports of these weapons.

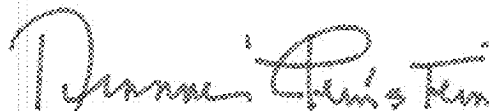
Combat rifles, including those commonly known as “sniper rifles” should not be removed from the USML, nor should rifles of any type that are U.S. military-standard 5.56 (and especially .50 caliber). Semi-automatic firearms should also not be removed, and neither should related equipment or ammunition or associated manufacturing equipment, technology, or technical data.

Thank you for your attention to our concerns. We look forward to consulting with you on this matter.

Sincerely,



BENJAMIN L. CARDIN
United States Senator



DIANNE FEINSTEIN
United States Senator



PATRICK J. LEAHY
United States Senator



United States Department of State

Washington, D.C. 20520

DEC 27 2017

The Honorable
Benjamin Cardin
United States Senate
Washington, DC 20510

Dear Senator Cardin:

Thank you for your letter dated September 15 outlining your concerns regarding proposed changes to Categories I, II, and III of the U.S. Munitions List (USML) and the considered transfer of small arms, light weapons, and associated equipment and ammunition to the Commerce Control List (CCL) regulated by the Department of Commerce.

We appreciate your support for the Export Control Reform Initiative efforts, which have rationalized and streamlined the United States Munitions List (USML) and made it easier for American small businesses to understand the relevant rules and successfully compete in the global marketplace.

The Department of State recognizes the sensitivities and foreign policy implications associated with the sale and export of small arms, light weapons, and associated equipment and ammunition. The deliberative interagency review process to consider potential changes to the treatment of Categories I, II, and III is identical to the approach that was applied to prior reviews of other USML categories.

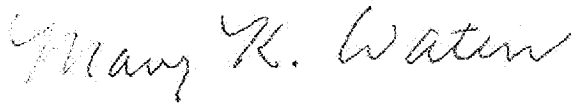
The proposed rules are currently being reviewed by the interagency, led by the Office of Management and Budget, and will then be published in the Federal Register with a request for public comment. Additionally, no significant changes to the content of Categories I, II, and III will occur until any final rules moving such items from the USML to the Commerce Control List are published. State will notify Congress in accordance with section 38(f) of the Arms Export Control Act and offer additional briefings on the matter once the final rules have been approved by the interagency.

We refer you to the Department of Commerce, Bureau of Industry and Security (BIS) for more information regarding its implementation of export controls on firearms that may become subject to its jurisdiction. BIS may be reached at 202-482-2721.

-2-

We hope this information is useful. Please let us know if we can be helpful on this or any other issue now or in the future.

Sincerely,

A handwritten signature in cursive script, reading "Mary K. Watten".

Charles S. Faulkner
Bureau of Legislative Affairs



United States Department of State

Washington, D.C. 20520

DEC 27 2017

The Honorable
Patrick J. Leahy
United States Senate
Washington, DC 20510

Dear Senator Leahy:

Thank you for your letter dated September 15 outlining your concerns regarding proposed changes to Categories I, II, and III of the U.S. Munitions List (USML) and the considered transfer of small arms, light weapons, and associated equipment and ammunition to the Commerce Control List (CCL) regulated by the Department of Commerce.

We appreciate your support for the Export Control Reform Initiative efforts, which have rationalized and streamlined the United States Munitions List (USML) and made it easier for American small businesses to understand the relevant rules and successfully compete in the global marketplace.

The Department of State recognizes the sensitivities and foreign policy implications associated with the sale and export of small arms, light weapons, and associated equipment and ammunition. The deliberative interagency review process to consider potential changes to the treatment of Categories I, II, and III is identical to the approach that was applied to prior reviews of other USML categories.

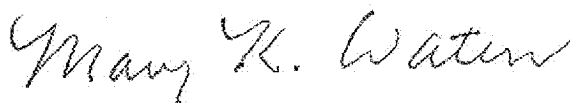
The proposed rules are currently being reviewed by the interagency, led by the Office of Management and Budget, and will then be published in the Federal Register with a request for public comment. Additionally, no significant changes to the content of Categories I, II, and III will occur until any final rules moving such items from the USML to the Commerce Control List are published. State will notify Congress in accordance with section 38(f) of the Arms Export Control Act and offer additional briefings on the matter once the final rules have been approved by the interagency.

We refer you to the Department of Commerce, Bureau of Industry and Security (BIS) for more information regarding its implementation of export controls on firearms that may become subject to its jurisdiction. BIS may be reached at 202-482-2721.

-2-

We hope this information is useful. Please let us know if we can be helpful on this or any other issue now or in the future.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mary K. Water".

Charles S. Faulkner
Bureau of Legislative Affairs



United States Department of State

Washington, D.C. 20520

DEC 27 2017

The Honorable
Dianne Feinstein
United States Senate
Washington, DC 20510

Dear Senator Feinstein:

Thank you for your letter dated September 15 outlining your concerns regarding proposed changes to Categories I, II, and III of the U.S. Munitions List (USML) and the considered transfer of small arms, light weapons, and associated equipment and ammunition to the Commerce Control List (CCL) regulated by the Department of Commerce.

We appreciate your support for the Export Control Reform Initiative efforts, which have rationalized and streamlined the United States Munitions List (USML) and made it easier for American small businesses to understand the relevant rules and successfully compete in the global marketplace.

The Department of State recognizes the sensitivities and foreign policy implications associated with the sale and export of small arms, light weapons, and associated equipment and ammunition. The deliberative interagency review process to consider potential changes to the treatment of Categories I, II, and III is identical to the approach that was applied to prior reviews of other USML categories.

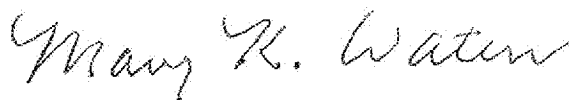
The proposed rules are currently being reviewed by the interagency, led by the Office of Management and Budget, and will then be published in the Federal Register with a request for public comment. Additionally, no significant changes to the content of Categories I, II, and III will occur until any final rules moving such items from the USML to the Commerce Control List are published. State will notify Congress in accordance with section 38(f) of the Arms Export Control Act and offer additional briefings on the matter once the final rules have been approved by the interagency.

We refer you to the Department of Commerce, Bureau of Industry and Security (BIS) for more information regarding its implementation of export controls on firearms that may become subject to its jurisdiction. BIS may be reached at 202-482-2721.

-2-

We hope this information is useful. Please let us know if we can be helpful on this or any other issue now or in the future.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mary K. Waten".

Charles S. Faulkner
Bureau of Legislative Affairs

Congress of the United States
Washington, DC 20515

September 22, 2017

The Honorable Rex Tillerson
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, D.C. 20520

The Honorable Wilbur Ross
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

RECEIVED
2017 OCT -3 P 4 15
LEGISLATIVE AFFAIRS

Dear Secretary Tillerson and Secretary Ross:

We are strong supporters of the Export Control Reform initiative (ECR) and respectfully urge you to complete it as soon as possible. Once finalized, it will save taxpayer dollars, create American jobs and strengthen our national security. The time to act is now for the completion of this critical initiative.

In 2009, a comprehensive review of the United States' export control system was undertaken with the goal of strengthening national security and the competitiveness of key domestic manufacturing and technology sectors. The review found that the current export control system is overly complicated and duplicative. This not only undermines the American economy, it also diminishes the ability of the United States government to focus its resources on the most critical national security priorities. Ultimately, the review led to the creation of ECR, which aimed to overhaul our nation's export control system.

A stated goal of ECR is, "Improving the long-term health and competitiveness of the U.S. industrial base, which includes maintaining and expanding jobs." While much of the work has been completed, there are still some important steps to take to ensure maximum efficiency. Categories one, two, and three of the United States Munitions List (USML) still need to be published as final rules. These three categories cover firearms, guns, and ammunition, which in turn affect the world-class firearm and ammunition manufacturers in Montana.

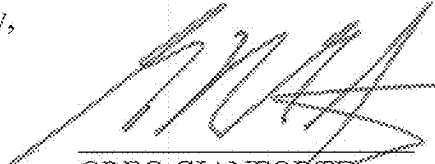
Thank you for your timely consideration of completing ECR. Finishing this much-needed reform will resolve unintended and unnecessary burdens currently placed on Montanan business and innovation, while also bolstering the security of the United States. We appreciate your efforts and look forward to seeing this commonsense initiative come to a prompt conclusion.

RM

Sincerely,

A handwritten signature in black ink that reads "Steve Daines". The signature is fluid and cursive, with the first name "Steve" and last name "Daines" clearly legible.

STEVE DAINES
United States Senator

A handwritten signature in black ink that reads "Greg Gianforte". The signature is bold and stylized, with the first name "Greg" and last name "Gianforte" clearly legible.

GREG GIANFORTE
Member of Congress



United States Department of State

Washington, D.C. 20520

OCT 20 2017

The Honorable
Steve Daines
United States Senate
Washington, DC 20510

Dear Senator Daines:

Thank you for your letter of September 22 expressing continued support for the Department's efforts to reform the U.S. export control system.

The Department of State has benefitted from the broad bipartisan support of Congress for our effort to modernize the U.S. export control system. With Congress's support, we have made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations and the Export Administration Regulations implemented by the Department of Commerce, and have revised 18 of the 21 Categories on the United States Munitions List (USML). The Department of State is seeking to conclude its initial review of the USML Categories and publish a proposed rule on the three remaining Categories: I, II, and III. These USML Categories currently control items including firearms, close assault weapons, and combat shotguns; guns and armament; and ammunition and ordnance.

The proposed rule is currently going through the interagency review process, under the coordination of the Office of Management and Budget. Once cleared for publication, the rule proposing revisions to these Categories will be published for public comment in the *Federal Register*, as the Department did for the previous rules proposing to revise the USML.

We hope you find this information helpful and appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in dark ink, appearing to read "Charles S. Faulkner".

Charles S. Faulkner
Bureau of Legislative Affairs



United States Department of State

Washington, D.C. 20520

OCT 20 2017

The Honorable
Greg Gianforte
House of Representatives
Washington, DC 20515

Dear Mr. Gianforte:

Thank you for your letter of September 22 expressing continued support for the Department's efforts to reform the U.S. export control system.

The Department of State has benefitted from the broad bipartisan support of Congress for our effort to modernize the U.S. export control system. With Congress's support, we have made progress toward clarifying and better harmonizing the International Traffic in Arms Regulations and the Export Administration Regulations implemented by the Department of Commerce, and have revised 18 of the 21 Categories on the United States Munitions List (USML). The Department of State is seeking to conclude its initial review of the USML Categories and publish a proposed rule on the three remaining Categories: I, II, and III. These USML Categories currently control items including firearms, close assault weapons, and combat shotguns; guns and armament; and ammunition and ordnance.

The proposed rule is currently going through the interagency review process, under the coordination of the Office of Management and Budget. Once cleared for publication, the rule proposing revisions to these Categories will be published for public comment in the *Federal Register*, as the Department did for the previous rules proposing to revise the USML.

We hope you find this information helpful and appreciate your interest in this important matter. Please do not hesitate to contact us with any additional questions.

Sincerely,

A handwritten signature in dark ink, appearing to read "Charles S. Faulkner".

Charles S. Faulkner
Bureau of Legislative Affairs

Billing Code 4710-25

DEPARTMENT OF STATE

22 CFR Parts 121, 123, 124, 126, and 129

[Public Notice 10094]

RIN 1400-AE30

Amendment to the International Traffic in Arms Regulations: Revision of U.S. Munitions List Categories I, II, and III

AGENCY: Department of State.

ACTION: Proposed rule.

SUMMARY: The Department of State (the Department) proposes to amend the International Traffic in Arms Regulations (ITAR) to revise Categories I (firearms, close assault weapons and combat shotguns), II (guns and armament) and III (ammunition and ordnance) of the U.S. Munitions List (USML) to describe more precisely the articles warranting export and temporary import control on the USML. Items removed from the USML would become subject to the Export Administration Regulations (EAR).

DATES: The Department will accept comments on this proposed rule until [insert date 45 days from date of publication in the *Federal Register*].

ADDRESSES:

Interested parties may submit comments within 45 days of the date of publication by one of the following methods:

- E-mail: DDTCPublicComments@state.gov with the subject line, “ITAR Amendment – Categories I, II, and III.”
- Internet: At www.regulations.gov, search for this notice by using this rule’s RIN (1400-AE30).

Comments received after that date will be considered if feasible, but consideration cannot be assured. Those submitting comments should not

include any personally identifying information they do not desire to be made public or information for which a claim of confidentiality is asserted, because those comments and/or transmittal e-mails will be made available for public inspection and copying after the close of the comment period via the Directorate of Defense Trade Controls website at *www.pmddtc.state.gov*. Parties who wish to comment anonymously may do so by submitting their comments via *www.regulations.gov*, leaving the fields that would identify the commenter blank and including no identifying information in the comment itself.

FOR FURTHER INFORMATION CONTACT: Robert Monjay, Office of Defense Trade Controls Policy, Department of State, telephone (202) 663-2817; e-mail *DDTCTPublicComments@state.gov*. ATTN: Regulatory Change, USML Categories I, II, and III.

SUPPLEMENTARY INFORMATION: The Directorate of Defense Trade Controls (DDTC), U.S. Department of State, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120-130). The items subject to the jurisdiction of the ITAR, *i.e.*, “defense articles,” are identified on the ITAR’s U.S. Munitions List (USML) (22 CFR 121.1). With few exceptions, items not subject to the export control jurisdiction of the ITAR are subject to the jurisdiction of the Export Administration Regulations (EAR, 15 CFR parts 730-774, which includes the Commerce Control List (CCL) in Supplement No. 1 to part 774), administered by the Bureau of Industry and Security (BIS), U.S. Department of Commerce. Both the ITAR and the EAR impose license requirements on exports and reexports. The Department of Commerce is publishing a companion rule in this edition of the *Federal Register*.

Pursuant to section 38(a)(1) of the Arms Export Control Act (AECA), all defense articles controlled for export or import are part of the United States Munitions List under the AECA. All references to the USML in this rule, however, are to the list of AECA defense articles that are controlled for purposes of export or temporary import pursuant to the ITAR, and not to the list of AECA defense articles on the United States Munitions Import List (USMIL) that are controlled by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) for purposes of permanent import under its regulations at 27 CFR Part 447. References to the USMIL are to the list of AECA defense articles controlled by ATF for purposes of permanent import.

Section 38(b)(1)(A)(ii) of the AECA, requires, with limited exceptions, registration of persons who engage in the business of brokering activities with respect to the manufacture, export, import, or transfer of any defense article or defense service designated by the President as such under section 38(a)(1) and licensing for such activities. Through Executive Order 13637, the President delegated the responsibility for registration and licensing of brokering activities to the Department of State with respect to defense articles or defense services controlled either for purposes of export by the Department of State or for purposes of permanent import by ATF. Section 129.1(b) of the ITAR states this requirement. As such, all defense articles described in the USMIL or the USML are subject to the brokering controls administered by the U.S. Department of State in part 129 of the ITAR. The transfer of defense articles from the ITAR's USML to the EAR's CCL for purposes of export controls does not affect the list of defense articles controlled on the USMIL under the AECA for purposes of permanent import or brokering controls for any brokering activity, including

facilitation in their manufacture, export, permanent import, transfer, reexport, or retransfer. This rule proposes adding a new paragraph (b)(2)(vii) to section 129.2 to update the enumerated list of actions that are not considered brokering. This change is a conforming change and is needed to address the movement of items from the USML to the CCL that will be subject to the brokering controls, to ensure that the US government does not impose a double licensing requirement on the export, reexport or retransfer of such items.

The Department of State is engaged in an effort to revise the U.S. Munitions List so that its scope is limited to those defense articles that provide the United States with a critical military or intelligence advantage or, in the case of weapons, are inherently for military end use. The articles now controlled by USML Categories I, II, and III that would be removed from the USML under this proposed rule do not meet this standard, including many items which are widely available in retail outlets in the United States and abroad.

Revision of Category I

This proposed rule revises USML Category I, covering firearms and related articles, to control only defense articles that are inherently military or that are not otherwise widely available for commercial sale. In particular, the revised category will not include non-automatic and semi-automatic firearms to caliber .50 (12.7mm) inclusive, currently controlled under paragraph (a), and all of the parts, components, accessories, and attachments specially designed for those articles. Such items will be subject to the new controls in Export Control Classification Numbers 0A501, 0A502, 0A503, 0A504, 0A505, 0B501, 0B505, 0D501, 0D505, 0E501, and 0E502. Such controls in

Category 0 of the CCL will be published in a separate rule by the Department of Commerce.

Paragraph (a) of USML Category I will cover firearms that fire caseless ammunition. Paragraph (b) will continue to cover fully automatic firearms to caliber .50 (12.7mm) inclusive. Paragraph (c) will cover firearms specially designed to integrate fire control, automatic tracking, or automatic firing systems, and all weapons previously described in paragraph (c) that remain on the USML will be covered by paragraph (a), (b) or (c) of this category or by Category II. Paragraph (d) will cover fully automatic shotguns. Paragraph (e) will continue to cover silencers, mufflers, sound suppressors, and specially designed parts and components; flash suppressors will be subject to the EAR. Paragraph (f) will be reserved, as riflescopes and other firearms sighting devices may be controlled in USML Category XII if they have night vision or infrared capabilities, and other riflescopes will be subject to the EAR. Paragraph (g) will continue to cover barrels, receivers (frames), bolts, bolt carriers, slides, or sears, specially designed for the firearms in Category I. Paragraph (h) will cover high capacity (greater than 50 rounds) magazines, and parts and components to convert a semi-automatic firearm into a fully automatic firearm, and accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting. Paragraph (i) will continue to cover the technical data and defense services.

A new (x) paragraph will be added to USML Category I, allowing ITAR licensing for commodities, software, and technology subject to the EAR, provided those commodities, software, and technology are to be used

in or with defense articles controlled in USML Category I *and* are described in the purchase documentation submitted with the license application.

The note to Category I will be retained, with conforming revisions. A new second note will be added to clarify the terms “firearm,” “fully automatic,” and “caseless ammunition”.

Revision of Category II

This proposed rule revises USML Category II, covering guns and armament, establishing a bright line between the USML and the CCL for the control of these articles.

Most significantly, paragraph (j), controlling parts and components, will be revised to enumerate the articles controlled therein.

Paragraph (a) will be revised to enumerate the articles controlled in that paragraph. The articles currently covered in paragraph (c) (apparatus and devices for launching or delivering ordnance) still warranting control on the ITAR will be included in new paragraph (a)(4). A new paragraph (a)(5) will be added for developmental guns and armaments funded by the Department of Defense and the specially designed parts and components of those developmental guns and armaments. The articles currently controlled in paragraph (f), engines for self-propelled guns and howitzers in paragraph (a), will be on the CCL in ECCN 0A606. Tooling and equipment for the production of articles controlled in USML Category II, currently in paragraph (g), will be on the CCL in ECCN 0B602. Test and evaluation equipment, currently in paragraph (h), will be on the CCL in ECCN 0B602. Certain autoloading systems controlled in paragraph (i) will be moved to paragraphs (j)(9) and (j)(11).

A new (x) paragraph will be added to USML Category II, allowing ITAR licensing for commodities, software, and technology subject to the EAR, provided those commodities, software, and technology are to be used in or with defense articles controlled in USML Category II *and* are described in the purchase documentation submitted with the application.

Revision of Category III

This proposed rule revises USML Category III, covering ammunition and ordnance, to establish a bright line between the USML and the CCL for the control of these articles and to be consistent with the changes to Category I.

Most significantly, paragraphs (a) and (d) will be revised to remove broad catch-alls and enumerate the articles to be controlled therein. For example, paragraph (a), which controls ammunition for articles in USML Categories I and II, will be revised to specifically list the ammunition that it controls. A new paragraph (a)(10) will be added for developmental ammunition funded by the Department of Defense and the parts and components specially designed for such developmental ammunition. Ammunition not enumerated in paragraph (a) will be subject to the EAR. Likewise, revised paragraph (d), which controls parts and components, will enumerate the articles it controls; those articles not identified but currently captured via the catch-all will be subject to the EAR.

Additionally, paragraph (c), which controls production equipment and tooling, will be removed and placed into reserve. The articles currently covered by this paragraph will be subject to the EAR.

A new (x) paragraph will be added to USML Category III, allowing ITAR licensing for commodities, software, and technology subject to the

EAR, provided those commodities, software, and technology are to be used in or with defense articles controlled in USML Category III *and* are described in the purchase documentation submitted with the application.

Conforming ITAR Changes

Additionally, conforming changes will be made to several sections of the ITAR that refer to the current controls in USML Category I(a). These sections will be amended because they all refer to firearms that will be controlled on the CCL. Section 123.16(b)(2) will be revised to remove reference to the firearms exemptions at §123.17, as the paragraphs in that section (a) through (e) that describe the firearms exemptions will be removed as a consequence of the control of non-automatic and semi-automatic firearms on the CCL. For the same reason, §123.16(b)(6) will be revised to describe only the remaining exemption at §123.17 (personal protective gear), and §123.16(b)(7) will be reserved. Section 123.17 will be amended to remove subparagraphs (a) through (e), consistent with changes made to the USML. Section 123.18, as it describes exemptions for firearms that will be controlled for export by the Department of Commerce, will be removed and placed into reserve. Revision of §124.14(c)(9) will remove the example of “sporting firearms for commercial resale.” The policy guidance on Zimbabwe in §126.1(s) will be revised to remove reference to the firearms exemption in §123.17.

Section 129.1(b) of the ITAR will be revised to clarify that the regulations on brokering activities in part 129 apply to those defense articles and defense services designated as such on the USML and those items described on the USMIL (27 CFR 447.21). Section 129.4 of the ITAR will also be revised to clarify brokering requirements for items on the USMIL

that are subject to the brokering requirements of the AECA. The items that will move to the CCL for export control purposes, yet are on the USMIL for permanent import purposes, remain subject to the brokering requirements of part 129 with respect to all brokering activities, including facilitation in their manufacture, export, permanent import, transfer, reexport, or retransfer. The revisions also clarify that foreign defense articles that are on the USMIL require brokering authorizations.

Request for Comments

The Department welcomes comments from the public and specifically requests input on the following matters:

- 1) A key goal of this rulemaking is to ensure the USML and the CCL together control all the items that meet Wassenaar Arrangement commitments embodied in its Munitions List Categories 1, 2 and 3 (WA-ML1, WA-ML2 and WA-ML3). Readers are asked to identify any potential gap in coverage brought about by the changes for USML Categories I, II and III contained in this notice and the new Category 0, 0x5zz ECCNs published separately by the Department of Commerce when reviewed together.
- 2) The Department seeks to establish clear distinctions between the USML and the CCL for the control of firearms, large guns, armaments, ordnance and ammunition. The public should provide any specific examples of firearms (or parts, components, accessories thereof), large guns, armaments, ordnance or ammunition whose jurisdiction is unclear based on this revision.
- 3) The Department has, in the past, adopted a delayed effective date of 180 days for rules revising entire categories of the USML and moving items to the CCL. The Department seeks to allow industry sufficient time to implement this rule, including time to make changes to IT systems,

technology controls plans, and other business processes. The public should provide input on the time necessary to implement any final rule for these categories, as well as a description of any increased burden that, in the view of the commenter, would be imposed on businesses or individuals should this rule be adopted.

REGULATORY ANALYSIS AND NOTICES

Administrative Procedure Act

The Department of State is of the opinion that controlling the import and export of defense articles and services is a foreign affairs function of the United States government and that rules implementing this function are exempt from sections 553 (rulemaking) and 554 (adjudications) of the Administrative Procedure Act (APA). Although the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of the APA and without prejudice to its determination that controlling the import and export of defense services is a foreign affairs function, the Department is publishing this proposed rule with a 45-day provision for public comment.

Regulatory Flexibility Act

Since the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of 5 U.S.C. 553, it does not require analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This proposed amendment does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions

were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

This rulemaking has been found not to be a major rule within the meaning of the Small Business Regulatory Enforcement Fairness Act of 1996.

Executive Orders 12372 and 13132

This rulemaking will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this rulemaking does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this rulemaking.

Executive Orders 12866 and 13563

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). The Department believes that the benefits of this rulemaking largely outweigh any costs, in that many items currently controlled on the more-restrictive USML are being moved to the CCL. We request comment from the public on any impact that would be imposed on the public if this rule were adopted.

Executive Order 13563 emphasizes the importance of considering both benefits and costs, both qualitative and quantitative, of harmonizing rules, and of promoting flexibility. This rule has been designated a “significant regulatory action,” although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget (OMB).

The Department believes the effect of this proposed rule would decrease the number of license applications submitted to the Department under OMB Control No. 1405-0003 by approximately 10,000 annually, for which the average burden estimates are one hour per form, which results in a burden reduction of 10,000 hours per year.

The Department of Commerce estimates that 4,000 of the 10,000 licenses that were required by the Department will be eligible for license exceptions or otherwise not require a separate license under the EAR. The Department of Commerce estimates that 6,000 transactions will require an individual validated license. The Department of Commerce will be collecting the information necessary to process license applications under OMB Control No. 0694-0088. The Department of Commerce estimates that OMB Control No. 0694-0088 takes approximately 43.8 minutes for a manual or electronic submission. The Department of Commerce estimates that the 6,000 licenses constitute a burden of 4,380 hours for this collection. The Department estimates a reduction in burden of 10,000 hours due to the proposed transition of these items to the Department of Commerce. The Department of Commerce estimates that the burden of submitting license applications for these items to the Department of Commerce will be 4,380 burden hours. Therefore, the net burden would be reduced by 5,620 hours.

The Department estimates that the burden hour cost for completing a license application is \$44.94 per hour. Therefore, the estimated net reduction of 5,620 burden hours per year is estimated to result in annual burden hour cost reduction of \$252,562.80. There may also be other State Department forms that will no longer need to be submitted and that may further reduce the burden hours for applicants. The Department is seeking comments on the reduction from the other forms, as referenced below.

In addition to the reduction in burden hours, there will be direct cost savings to the State Department that would result from the 10,000 license applications no longer being required under the ITAR once these items are moved to the EAR. Pursuant to the AECA, ITAR, and associated delegations of authority, every person who engages in the business of brokering activities, manufacturing, exporting, or temporarily importing any defense articles or defense services must register with the Department of State and pay a registration fee. The Department of State adopted the current fee schedule to align the registration fees with the cost of licensing, compliance and other related activities. The Department of Commerce would incur additional costs to administer these controls and process license applications. However, the Department of Commerce does not charge a registration fee to exporters under the EAR and we are unable to estimate the increase in costs to the Department of Commerce to process the new license applications. Therefore, we are unable to provide an estimate of the net change in resource costs to the government from moving these items from the ITAR to the EAR. It is the case, however, that the movement of these items from the ITAR would result in a direct transfer of \$2,500,000 per year from the government to the exporting public, less the increased cost to

taxpayers, because they would no longer pay fees to the State Department and there is no fee charged by the Department of Commerce to apply for a license.

The Department welcomes comments from the public on the net reduction in burden described within this section, particularly if there are additional burden reductions that are not reflected here (please provide number of hours or cost) or if the estimates noted here appear otherwise inaccurate.

Estimated cost savings

The Department of State is of the opinion that controlling the import and export of defense articles and services is a foreign affairs function of the United States government and that rules implementing this function are exempt from Executive Order 13771 (82 FR 9339, February 3, 2017).

Although the Department is of the opinion that this proposed rule is exempt from E.O. 13771 and without prejudice to its determination that controlling the import and export of defense services is a foreign affairs function, this proposed rule is expected to be an EO 13771 deregulatory action. The Department has conducted this analysis in close consultation with the Department of Commerce. The total annual recurring dollar cost savings is estimated to be \$1,376,281 for purposes of E.O. 13771 for the Department of State.

Executive Order 12988

The Department of State has reviewed this rulemaking in light of sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department of State has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, Executive Order 13175 does not apply to this rulemaking.

Paperwork Reduction Act

Notwithstanding any other provision of law, no person is required to respond to, nor is subject to a penalty for failure to comply with, a collection of information, subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid OMB control number.

The Department of State believes there would be a reduction in burden for OMB Control No. 1405-0003, Application/License for Permanent Export of Unclassified Defense Articles and Related Unclassified Technical Data. This form is an application that, when completed and approved by Department of State, constitutes the official record and authorization for the commercial export of unclassified U.S. Munitions List articles and technical data, pursuant to the AECA and ITAR. For an analysis of the reduction in burden for OMB Control No. 1405-0003, see the above Section for E.O. 12866. The Department of State requests comments on the collection of information or potential reduction in burden be sent also to the Office of Information and Regulatory Affairs of OMB, Attention: Desk Officer for Department of State, at OIRA_Submission@omb.eop.gov or Attention: Desk Officer for Department of State, Office of Information and Regulatory Affairs of OMB, 725 17th St NW, Washington, D.C. 20503.

List of Subjects in Parts 121, 123, 124, 126, and 129

Arms and munitions, Exports

Accordingly, for the reasons set forth above, Title 22, Chapter I, Subchapter M, parts 121, 123, 124, 126, and 129 are proposed to be amended as follows:

PART 121 – THE UNITED STATES MUNITIONS LIST

1. The authority citation for part 121 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; Pub. L. 105–261, 112 Stat. 1920; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

2. Section 121.1 is amended by revising U.S. Munitions List Categories I, II, and III to read as follows:

§121.1 The United States Munitions List.

I—Firearms and Related Articles

- *(a) Firearms using caseless ammunition.
- *(b) Fully automatic firearms to .50 caliber (12.7 mm) inclusive.
- *(c) Firearms specially designed to integrate fire control, automatic tracking, or automatic firing (e.g., Precision Guided Firearms (PGFs)), and specially designed parts and components therefor.

Note to paragraph (c): Integration does not include only attaching to the firearm or rail.

- *(d) Fully automatic shotguns regardless of gauge.
- *(e) Silencers, mufflers, and sound suppressors, and specially designed parts and components therefor.
- (f) [Reserved]
- (g) Barrels, receivers (frames), bolts, bolt carriers, slides, or sears specially designed for the articles in paragraphs (a), (b), and (d) of this category.

(h) Parts, components, accessories, and attachments, as follows:

(1) Drum and other magazines for firearms to .50 caliber (12.7 mm) inclusive with a capacity greater than 50 rounds, regardless of jurisdiction of the firearm, and specially designed parts and components therefor;

(2) Parts and components specially designed for conversion of a semi-automatic firearm to a fully automatic firearm.

(3) Accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting, and specially designed parts and components therefor.

(i) Technical data (*see* §120.10 of this subchapter) and defense services (*see* §120.9 of this subchapter) directly related to the defense articles described in paragraphs (a), (b), (d), (e), (g), and (h) of this category and classified technical data directly related to items controlled in ECCNs 0A501, 0B501, 0D501, and 0E501 and defense services using the classified technical data. (*See* §125.4 of this subchapter for exemptions.)

(j)-(w) [Reserved]

(x) Commodities, software, and technology subject to the EAR (*see* §120.42 of this subchapter) used in or with defense articles.

Note to paragraph (x): Use of this paragraph is limited to license applications for defense articles where the purchase documentation includes commodities, software, or technology subject to the EAR (*see* §123.1(b) of this subchapter).

Note 1 to Category I: Paragraphs (a), (b), (d), (e), (g), (h), and (i) of this category exclude: any non-automatic or semi-automatic firearms to .50 caliber (12.7 mm) inclusive; non-automatic shotguns; BB, pellet, and muzzle loading (*e.g.*, black powder) firearms; and parts, components, accessories,

and attachments of firearms and shotguns in paragraph (a), (b), (d), and (g) of this category that are common to non-automatic firearms and shotguns. The Department of Commerce regulates the export of such items. See the Export Administration Regulations (15 CFR parts 730-774).

Note 2 to Category I: The following interpretations explain and amplify the terms used in this category:

- (1) A firearm is a weapon not over .50 caliber (12.7 mm) which is designed to expel a projectile by the deflagration of propellant.
- (2) A fully automatic firearm or shotgun is any firearm or shotgun which shoots, is designed to shoot, or can readily be restored to shoot, automatically more than one shot, without manual reloading, by a single function of the trigger.
- (3) Caseless ammunition is firearm ammunition without a cartridge case that holds the primer, propellant, and projectile together as a unit.

Category II— Guns and Armament

(a) Guns and armament greater than .50 caliber (12.7 mm), as follows:

- *(1) Guns, howitzers, artillery, and cannons;
- *(2) Mortars;
- *(3) Recoilless rifles;
- *(4) Grenade launchers; or
- (5) Developmental guns and armament greater than .50 caliber (12.7 mm) funded by the Department of Defense and specially designed parts and components therefor.

Note 1 to paragraph (a)(5): This paragraph does not control guns and armament greater than .50 caliber (12.7 mm) (a) in production, (b) determined to be subject to the EAR via a commodity jurisdiction

determination (*see* §120.4 of this subchapter), or (c) identified in the relevant Department of Defense contract or other funding authorization as being developed for both civil and military applications.

Note 2 to paragraph (a)(5): Note 1 does not apply to defense articles enumerated on the U.S. Munitions List, whether in production or development.

Note 3 to paragraph (a)(5): This provision is applicable to those contracts or other funding authorizations that are dated (one year after publication of the final rule), or later.

Note 1 to paragraph (a): This paragraph does not include: Non-automatic and non-semi-automatic rifles, carbines, and pistols between .50 (12.7 mm) and .72 caliber (18.288 mm) that are controlled on the CCL under ECCN 0A501; shotguns controlled on the CCL under ECCN 0A502; or black powder guns and armaments manufactured between 1890 and 1919 controlled on the CCL under ECCN 0A602.

Note 2 to paragraph (a): Guns and armament when integrated into their carrier (*e.g.*, ships, ground vehicles, or aircraft) are controlled in the category associated with the carrier. Self-propelled guns and armament are controlled in USML Category VII. Towed guns and armament and stand-alone guns and armament are controlled under this category.

(b) Flame throwers with a minimum effective range of 20 meters.

(c) [Reserved]

*(d) Kinetic energy weapon systems specially designed for destruction or rendering mission-abort of a target.

Note to paragraph (d): Kinetic energy weapons systems include but are not limited to launch systems and subsystems capable of accelerating masses

larger than 0.1g to velocities in excess of 1.6 km/s, in single or rapid fire modes, using methods such as: electromagnetic, electrothermal, plasma, light gas, or chemical. This does not include launch systems and subsystems used for research and testing facilities subject to the EAR, which are controlled on the CCL under ECCN 2B232.

(e) Signature reduction devices specially designed for the guns and armament controlled in paragraphs (a), (b), and (d) of this category (*e.g.*, muzzle flash suppression devices).

(f)-(i) [Reserved]

(j) Parts, components, accessories, and attachments, as follows:

- (1) Gun barrels, rails, tubes, and receivers specially designed for the weapons controlled in paragraphs (a) and (d) of this category;
- (2) Sights specially designed to orient indirect fire weapons;
- (3) Breech blocks for the weapons controlled in paragraphs (a) and (d) of this category;
- (4) Firing mechanisms for the weapons controlled in paragraphs (a) and (d) of this category and specially designed parts and components therefor;
- (5) Systems for firing superposed or stacked ammunition and specially designed parts and components therefor;
- (6) Servo-electronic and hydraulic elevation adjustment mechanisms;
- (7) Muzzle brakes;
- (8) Bore evacuators;
- (9) Independently powered ammunition handling systems and platform interface components as follows:
 - (i) Mounts;
 - (ii) Carriages;

- (iii) Gun pallets;
- (iv) Hydro-pneumatic equilibration cylinders; or
- (v) Hydro-pneumatic systems capable of scavenging recoil energy to power howitzer functions;

Note to paragraph (j)(9): For weapons mounts specially designed for ground vehicles, *see* Category VII.

- (10) Recoil systems to mitigate the shock associated with the firing process of guns integrated into air platforms and specially designed parts and components therefor;
- (11) Independent ammunition handling systems for the guns and armament controlled in paragraphs (a), (b), and (d) of this category;
- (12) Ammunition containers/drums, ammunition chutes, ammunition conveyor elements, and ammunition container/drum entrance and exit units, specially designed for the guns and armament controlled in paragraphs (a), (b), and (d) of this category;
- (13) Aircraft/gun interface units to support gun systems with a designed rate of fire greater than 100 rounds per minute and specially designed parts and components therefor;
- (14) Prime power generation, energy storage, thermal management, conditioning, switching, and fuel-handling equipment, and the electrical interfaces between the gun power supply and other turret electric drive components specially designed for kinetic weapons controlled in paragraph (d) of this category;
- (15) Kinetic energy weapon target acquisition, tracking fire control, and damage assessment systems and specially designed parts and components therefor; or

*(16) Any part, component, accessory, attachment, equipment, or system that:

- (i) Is classified;
- (ii) Contains classified software; or
- (iii) Is being developed using classified information.

“Classified” means classified pursuant to Executive Order 13526, or predecessor order, and a security classification guide developed pursuant thereto or equivalent, or to the corresponding classification rules of another government or intergovernmental organization.

(k) Technical data (*see* §120.10 of this subchapter) and defense services (*see* §120.9 of this subchapter) directly related to the defense articles described in paragraphs (a), (b), (d), (e), and (j) of this category and classified technical data directly related to items controlled in ECCNs 0A602, 0B602, 0D602, and 0E602 and defense services using the classified technical data. (*See* §125.4 of this subchapter for exemptions.)

(l)-(w) [Reserved]

(x) Commodities, software, and technology subject to the EAR (*see* §120.42 of this subchapter) used in or with defense articles.

Note to paragraph (x): Use of this paragraph is limited to license applications for defense articles where the purchase documentation includes commodities, software, or technology subject to the EAR (*see* §123.1(b) of this subchapter).

Category III — Ammunition and Ordnance

*(a) Ammunition, as follows:

- (1) Ammunition that incorporates a projectile controlled in paragraphs (d)(1) or (d)(3) of this category;

- (2) Ammunition preassembled into links or belts;
- (3) Shotgun ammunition that incorporates a projectile controlled in paragraph (d)(2) of this category;

- (4) Caseless ammunition manufactured with smokeless powder;

Note to paragraph (a)(4): Caseless ammunition is ammunition without a cartridge case that holds the primer, propellant, and projectile together as a unit.

- (5) Ammunition, except shotgun ammunition, based on non-metallic cases, or non-metallic cases that have only a metallic base, which result in a total cartridge mass 80% or less than the mass of a brass- or steel-cased cartridge that provides comparable ballistic performance;

- (6) Ammunition employing pyrotechnic material in the projectile base and any ammunition employing a projectile that incorporates tracer materials of any type having peak radiance above 710 nm and designed to be observed primarily with night vision optical systems;

- (7) Ammunition for fully automatic firearms or guns that fire superposed or stacked projectiles;

- (8) Electromagnetic armament projectiles or billets for weapons with a design muzzle energy exceeding 5 MJ;

- (9) Ammunition, not specified above, for the guns and armaments controlled in Category II; or

- (10) Developmental ammunition funded by the Department of Defense and specially designed parts and components therefor.

Note 1 to paragraph (a)(10): This paragraph does not control ammunition

(a) in production, (b) determined to be subject to the EAR via a commodity jurisdiction determination (*see* §120.4 of this subchapter), or (c) identified in

the relevant Department of Defense contract or other funding authorization as being developed for both civil and military applications.

Note 2 to paragraph (a)(10): Note 1 does not apply to defense articles enumerated on the U.S. Munitions List, whether in production or development.

Note 3 to paragraph (a)(10): This provision is applicable to those contracts or other funding authorizations that are dated (one year after publication of the final rule), or later.

(b) Ammunition/ordnance handling equipment specially designed for the articles controlled in this category, as follows:

(1) Belting, linking, and de-linking equipment; or

(2) Fuze setting devices.

(c) [Reserved]

(d) Parts and components for the articles in this category, as follows:

(1) Projectiles that use pyrotechnic tracer materials that incorporate any material having peak radiance above 710 nm or are incendiary, explosive, steel tipped, or contain a core or solid projectile produced from one or a combination of the following: tungsten, steel, or beryllium copper alloys;

(2) Shotgun projectiles that are flechettes, incendiary, tracer, or explosive;

Note to paragraph (d)(2): This paragraph does not include explosive projectiles specially designed to produce noise for scaring birds or other pests (*e.g.*, bird bombs, whistlers, crackers).

(3) Projectiles of any caliber produced from depleted uranium;

(4) Projectiles not specified above, guided or unguided, for the items controlled in USML Category II, and specially designed parts and components therefor (*e.g.*, fuzes, rotating bands, cases, liners, fins, boosters);

(5) Canisters or sub-munitions (*e.g.*, bomblets or minelets), and specially designed parts and components therefor, for the guns or armament controlled in USML Category II;

(6) Hardened cores, regardless of caliber, produced from one or a combination of the following: tungsten, steel, or beryllium copper alloy;

(7) Cartridge cases, powder bags, or combustible cases for the items controlled in USML Category II;

(8) Non-metallic cases, including cases that have only a metallic base, for the ammunition controlled in paragraph (a)(5) of this category;

(9) Cartridge links and belts for fully automatic firearms and guns controlled in USML Categories I or II;

(10) Primers other than Boxer, Berdan, or shotshell types;

Note to paragraph (d)(10): This paragraph does not control caps or primers of any type in use prior to 1890.

(11) Safing, arming, and fuzing components (to include target detection and proximity sensing devices) for the ammunition in this category and specially designed parts therefor;

(12) Guidance and control components for the ammunition in this category and specially designed parts therefor;

(13) Terminal seeker assemblies for the ammunition in this category and specially designed parts and components therefor;

(14) Illuminating flares or target practice projectiles for the ammunition controlled in paragraph (a)(9) of this category; or

*(15) Any part, component, accessory, attachment, equipment, or system that:

(i) Is classified;

- (ii) Contains classified software; or
- (iii) Is being developed using classified information.

“Classified” means classified pursuant to Executive Order 13526, or predecessor order, and a security classification guide developed pursuant thereto or equivalent, or to the corresponding classification rules of another government or intergovernmental organization.

(e) Technical data (*see* §120.10 of this subchapter) and defense services (*see* §120.9 of this subchapter) directly related to the defense articles enumerated in paragraphs (a), (b), and (d) of this category and classified technical data directly related to items controlled in ECCNs 0A505, 0B505, 0D505, and 0E505 and defense services using the classified technical data. (*See* §125.4 of this subchapter for exemptions.).

(f)-(w) [Reserved]

(x) Commodities, software, and technology subject to the EAR (*see* §120.42 of this subchapter) used in or with defense articles.

Note to paragraph (x): Use of this paragraph is limited to license applications for defense articles where the purchase documentation includes commodities, software, or technology subject to the EAR (*see* §123.1(b) of this subchapter).

Notes to Category III:

1. This category does not control ammunition crimped without a projectile (blank star) and dummy ammunition with a pierced powder chamber.
2. This category does not control cartridge and shell casings that, prior to export, have been rendered useless beyond the possibility of restoration for use as a cartridge or shell casing by means of heating, flame treatment, mangling, crushing, cutting, or popping.

3. Grenades containing non-lethal or less lethal projectiles are under the jurisdiction of the Department of Commerce.

* * * * *

PART 123 – LICENSES FOR THE EXPORT OF DEFENSE ARTICLES

3. The authority citation for part 123 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2753; 22 U.S.C. 2651a; 22 U.S.C. 2776; Pub. L. 105–261, 112 Stat. 1920; Sec 1205(a), Pub. L. 107–228; Sec. 520, Pub. L. 112-55; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

4. Section 123.15 is amended by revising paragraph (a)(3), as follows:

§ 123.15 Congressional certification pursuant to Section 36(c) of the Arms Export Control Act.

(a) * * *

(3) A license for export of defense articles controlled under Category I paragraphs (a) through (g) of the United States Munitions List, of this subchapter, in an amount of \$1,000,000 or more.

* * * * *

5. Section 123.16 is amended by revising paragraphs (b)(2) and (b)(6), and by removing paragraph (b)(7) and placing it in reserve, as follows:

§123.16 Exemptions of general applicability.

* * * * *

(b) * * *

(2) Port Directors of U.S. Customs and Border Protection shall permit the export of parts or components without a license when the total value does not exceed \$500 in a single transaction and:

* * * * *

(6) For exemptions for personal protective gear, refer to §123.17 of this subchapter.

(7) [Reserved]

* * * * *

6. Section 123.17 is amended by revising the section heading, and removing paragraphs (a) through (e) and placing them in reserve and by revising paragraph (j), as follows:

§123.17 Exemption for personal protective gear.

(a) – (e) [Reserved]

* * * * *

(j) If the articles temporarily exported pursuant to paragraphs (f) through (i) of this section are not returned to the United States, a detailed report must be submitted to the Office of Defense Trade Controls Compliance in accordance with the requirements of § 127.12(c)(2) of this subchapter.

* * * * *

7. Section 123.18 is removed and reserved.

§123.18 [Reserved]

PART 124 – AGREEMENTS, OFF-SHORE PROCUREMENT, AND OTHER DEFENSE SERVICES

8. The authority citation for part 124 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; 22 U.S.C. 2776; Section 1514, Pub. L. 105–261; Pub. L. 111-266; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

9. Section 124.14 is amended by revising paragraph (c)(9) to read as

follows:

§124.14 Exports to warehouses or distribution points outside the United States.

* * * * *

(c) * * *

(9) Additional clause. Unless the articles covered by the agreement are in fact intended to be distributed to private persons or entities (*e.g.*, cryptographic devices and software for financial and business applications), the following clause must be included in all warehousing and distribution agreements: “Sales or other transfers of the licensed article shall be limited to governments of the countries in the distribution territory and to private entities seeking to procure the licensed article pursuant to a contract with a government within the distribution territory, unless the prior written approval of the U.S. Department of State is obtained.”

* * * * *

PART 126 – GENERAL POLICIES AND PROVISIONS

10.The authority citation for part 126 continues to read as follows:

Authority: Secs. 2, 38, 40, 42 and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2780, 2791 and 2797); 22 U.S.C. 2651a; 22 U.S.C. 287c; E.O. 12918, 59 FR 28205; 3 CFR, 1994 Comp., p.899; Sec. 1225, Pub. L. 108–375; Sec. 7089, Pub. L. 111-117; Pub. L. 111-266; Section 7045, Pub. L. 112-74; Section 7046, Pub. L. 112-74; E.O. 13637, 78 FR 16129.

11.Section 126.1 is amended by revising paragraph (s) to read as follows:

§126.1 Prohibited exports, imports, and sales to or from certain countries.

* * * * *

(s) *Zimbabwe*. It is the policy of the United States to deny licenses or other approvals for exports or imports of defense articles and defense services destined for or originating in Zimbabwe, except that a license or other approval may be issued, on a case-by-case basis, for the temporary export of firearms and ammunition for personal use by individuals (not for resale or retransfer, including to the Government of Zimbabwe).

* * * * *

PART 129 -- REGISTRATION AND LICENSING OF BROKERS

12. The authority citation for part 129 continues to read as follows:

Authority: Section 38, Pub. L. 104-164, 110 Stat. 1437, (22 U.S.C. 2778); E.O. 13637, 78 FR 16129.

13. Section 129.1 is amended by revising paragraph (b) to read as follows:

§129.1 Purpose.

* * * * *

(b) All brokering activities identified in this subchapter apply equally to those defense articles and defense services designated in § 121.1 of this subchapter and those items designated in 27 CFR 447.21 (U.S. Munitions Import List).

14. Section 129.2 is amended by revising paragraph (b)(2)(v) by removing the word “or” at the end of the paragraph, adding the word “or” at the end of paragraph (b)(2)(vi), and adding a new paragraph (b)(2)(vii), to read as follows:

§129.2 Definitions.

* * * * *

(b) * * *

(2) * * *

(vii) Activities by persons to facilitate the export, reexport, or transfer of an item subject to the EAR that has been approved pursuant to a license or license exception under the EAR or a license or other approval under this subchapter.

15. Section 129.4 is amended by revising paragraphs (a)(1) and (a)(2)(i), to read as follows:

§129.4 Requirement for approval.

(a) * * *

(1) Any foreign defense article or defense service enumerated in part 121 of this subchapter (see §120.44 of this subchapter, and §129.5 for exemptions) and those foreign origin items on the U.S. Munitions Import List (*see* 27 CFR 447.21); or

(2) * * *

(i) Firearms and other weapons of a nature described by Category I(a) through (d), Category II(a) and (d), and Category III(a) of §121.1 of this subchapter or Category I(a) through (c), Category II(a), and Category III(a) of the U.S. Munitions Import List (*see* 27 CFR 447.21);

* * * * *

16. Section 129.6 is amended by revising paragraph (b)(3)(i), to read as follows:

§129.6 Procedures for obtaining approval.

* * * * *

(b) * * *

(3) * * *

(i) The U.S. Munitions List or U.S. Munitions Import List (*see* 27 CFR 447.21) category and sub-category for each article;

* * * * *

8A002 Marine systems, equipment, “parts” and “components,” as follows (see List of Items Controlled).

* * * * *

List of Items Controlled

* * * * *

Related Controls: (1) See also 8A992 and for underwater communications systems, see Category 5, Part I—Telecommunications. (2) See also 8A992 for self-contained underwater breathing apparatus that is not controlled by 8A002 or released for control by the 8A002.q Note. (3) For electronic imaging systems “specially designed” or modified for underwater use incorporating image intensifier tubes specified by 6A002.a.2.a or 6A002.a.2.b, see 6A003.b.3. (4) For electronic imaging systems “specially designed” or modified for underwater use incorporating “focal plane arrays” specified by 6A002.a.3.g, see 6A003.b.4.c. (5) Section 744.9 imposes a license requirement on commodities described in 8A002.d.1.c or .d.2 if being exported, reexported, or transferred (in-country) for use by a military end-user or for incorporation into an item controlled by ECCN 0A919.

* * * * *

Dated: April 16, 2015.

Kevin J. Wolf,

Assistant Secretary of Commerce for Export Administration.

[FR Doc. 2015–10353 Filed 5–4–15; 8:45 am]

BILLING CODE 3510–33–P

DEPARTMENT OF STATE

22 CFR Part 121

[Public Notice: 9110]

RIN 1400–AD32

Amendment to the International Traffic in Arms Regulations: Revision of U.S. Munitions List Category XII

AGENCY: Department of State.

ACTION: Proposed rule.

SUMMARY: As part of the President’s Export Control Reform effort, the Department of State proposes to amend the International Traffic in Arms Regulations (ITAR) to revise Category XII (fire control, range finder, optical and guidance and control equipment) of the U.S. Munitions List (USML) to describe more precisely the articles warranting control on the USML.

DATES: The Department of State will accept comments on this proposed rule until July 6, 2015.

ADDRESSES: Interested parties may submit comments within 60 days of the date of publication by one of the following methods:

- *Email:* DDTCPublicComments@state.gov with the subject line, “ITAR Amendment—Category XII.”

- *Internet:* At www.regulations.gov, search for this notice by using this rule’s RIN (1400–AD32).

Comments received after that date will be considered if feasible, but consideration cannot be assured. Those submitting comments should not include any personally identifying information they do not desire to be made public or any information for which a claim of confidentiality is asserted. All comments and transmittal emails will be made available for public inspection and copying after the close of the comment period via the Directorate of Defense Trade Controls Web site at www.pmdt.state.gov. Parties who wish to comment anonymously may do so by submitting their comments via www.regulations.gov, leaving the fields that would identify the commenter blank and including no identifying information in the comment itself. Comments submitted via www.regulations.gov are immediately available for public inspection.

FOR FURTHER INFORMATION CONTACT: Mr. C. Edward Peartree, Director, Office of Defense Trade Controls Policy, Department of State, telephone (202) 663–2792; email DDTCPublicComments@state.gov. ATTN: Regulatory Change, USML Category XII.

SUPPLEMENTARY INFORMATION: The Directorate of Defense Trade Controls (DDTC), U.S. Department of State, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120–130). The items subject to the jurisdiction of the ITAR, *i.e.*, “defense articles,” are identified on the ITAR’s U.S. Munitions List (USML) (22 CFR 121.1). With few exceptions, items not subject to the export control jurisdiction of the ITAR are subject to the jurisdiction of the Export Administration Regulations (“EAR,” 15 CFR parts 730–774, which includes the Commerce Control List (CCL) in Supplement No. 1 to Part 774), administered by the Bureau of Industry and Security (BIS), U.S. Department of Commerce. Both the ITAR and the EAR impose license requirements on exports and reexports. Items not subject to the ITAR or to the exclusive licensing jurisdiction of any other set of regulations are subject to the EAR. The revisions contained in this rule are part of the Department of State’s retrospective plan under E.O. 13563 completed on August 17, 2011. The Department of State’s full plan can be accessed at <http://www.state.gov/documents/organization/181028.pdf>.

Revision of Category XII

This proposed rule revises USML Category XII, covering fire control, range finder, optical and guidance and control equipment, to advance the national security objectives set forth above and to more accurately describe the articles within the category, in order to establish a “bright line” between the USML and the CCL for the control of these articles.

Paragraph (a) is revised to add subparagraphs (1) through (9) to more clearly describe the articles controlled in (a).

Paragraph (a)(1) is added for fire control systems and equipment.

Paragraph (a)(2) is added for weapons sights and weapons aiming or imaging systems, with certain infrared focal plane arrays, image intensifier tubes, ballistic computers, or lasers.

Paragraph (a)(3) is added for electronic or optical weapon positioning, laying, or spotting systems or equipment.

Paragraph (a)(4) is added for certain laser spot trackers and laser spot detectors.

Paragraph (a)(5) is added for bomb sights and bombing computers.

Paragraph (a)(6) is added for electro-optical missile or ordnance tracking or guidance systems.

Paragraph (a)(7) is added for electro-optical systems or equipment that automatically detect and locate weapons launch or fire.

Paragraph (a)(8) is added for certain remote wind sensing systems or equipment for enhanced targeting.

Paragraph (a)(9) is added for certain helmet mounted display (HMD) systems.

Paragraph (b) is revised to add subparagraphs (1) through (14) to more clearly describe the articles controlled in (b).

Paragraph (b)(1) is added for laser target designators or coded target markers.

Paragraph (b)(2) is added for certain infrared laser aiming or target illumination systems.

Paragraph (b)(3) is added for certain laser range finders.

Paragraph (b)(4) is added for certain targeting or target location systems.

Paragraph (b)(5) is added for optical augmentation systems.

Paragraph (b)(6) is added for certain light detection and ranging (LIDAR), laser detection and ranging (LADAR), or range-gated systems and includes a carve out for certain LIDAR systems for civil automotive applications.

Paragraph (b)(7) is added for certain synthetic aperture LIDAR or LADAR systems.

Paragraph (b)(8) is added for LIDAR, LADAR, or other laser range-gated identified in subparagraphs (i)–(vi).

Paragraph (b)(9) is added for certain lasers for electronic combat systems controlled in Category XI(a)(4).

Paragraph (b)(10) is added for certain tunable semiconductor lasers.

Paragraph (b)(11) is added for certain non-tunable single transverse mode semiconductor lasers.

Paragraph (b)(12) is added for certain non-tunable multiple transverse mode semiconductor lasers.

Paragraph (b)(13) is added for laser stacked arrays identified in subparagraphs (i)–(iv).

Paragraph (b)(14) is added for developmental lasers funded by the Department of Defense.

Paragraph (c) is revised to add subparagraphs (1) through (21) to more clearly describe the articles controlled in (c).

Paragraph (c)(1) is added for certain second and third generations image intensifier tubes (IITs).

Paragraph (c)(2) is added for certain photon detector, microbolometer detector, or multispectral detector infrared focal plane arrays (IRFPAs).

Paragraph (c)(3) is added for certain one-dimensional photon detector IRFPAs in a permanent encapsulated sensor assembly.

Paragraph (c)(4) is added for certain two-dimensional photon detector IRFPAs in a permanent encapsulated sensor assembly.

Paragraph (c)(5) is added for certain microbolometer IRFPAs in a permanent encapsulated sensor assembly.

Paragraph (c)(6) is added for multispectral IRFPAs in a permanent encapsulated sensor assembly.

Paragraph (c)(7) is added for certain charge multiplication focal plane arrays.

Paragraph (c)(8) is added for certain charge multiplication focal plane arrays in a permanent encapsulated sensor assembly.

Paragraph (c)(9) is added for certain integrated IRFPA dewar cooler assemblies (IDCAs).

Paragraph (c)(10) is added for gimbals with two or more axes of active stabilization having a minimum root-mean-square (RMS) stabilization better (less) than 200 microradians.

Paragraph (c)(11) is added for gimbals with two or more axes of active stabilization having a minimum root-mean-square (RMS) stabilization better (less) than 100 microradians.

Paragraph (c)(12) is added for infrared imaging camera cores identified in subparagraphs (i)–(xi). Camera cores meeting the shock tolerance criteria described in (c)(12)(ii) are controlled on

the USML whether or not they are tested to meet these criteria.

Paragraph (c)(13) is added for binoculars, bioculars, monoculars, goggles, or head- or helmet-mounted imaging systems with IITs or camera cores controlled in this category.

Paragraph (c)(14) is added for certain targeting systems.

Paragraph (c)(15) is added for infrared search and track (IRST) systems.

Paragraph (c)(16) is added for infrared imaging systems identified in subparagraphs (i)–(ix).

Paragraph (c)(17) is added for certain terahertz imaging systems.

Paragraph (c)(18) is added for near-to-eye display systems or equipment, specially designed for articles controlled in this subchapter.

Paragraph (c)(19) is added for systems or equipment that project radiometrically calibrated scenes directly into the entrance aperture of an electro-optical or infrared (EO/IR) sensor controlled in this subchapter within either the spectral band exceeding 10 nm but not exceeding 400 nm, or the spectral band exceeding 900 nm but not exceeding 30,000 nm.

Paragraph (c)(20) is added for certain systems or equipment incorporating an infrared beacon or emitter specially designed for Identification Friend or Foe (IFF) and specially designed parts and components therefor.

Paragraph (c)(21) is added for developmental imaging systems funded by the Department of Defense.

A note is added to paragraph (c) to address the incorporation of these defense articles into commercial items. With minor exceptions, all bare IRFPAs are controlled in Category XII, paragraph (c)(2). However, once an IRFPA has been incorporated into a permanent encapsulated sensor assembly, it ceases to be controlled in paragraph (c)(2) because it is incorporated into a higher order assembly. The permanent encapsulated sensor assembly will be controlled in paragraphs (c)(3)–(6), if it meets the control parameters of one of those paragraphs. These control parameters are set at a level that the Department has determined excludes most commercial products. Further, once most IRFPAs and permanent encapsulated sensor assemblies are incorporated into a camera core, monocular, or binocular or other higher order system, that system will not be subject to the ITAR or require authorization from the Department for export, unless it is specifically enumerated. Most multi-spectral IRFPAs and IRFPAs with charge multiplication are excluded from the note and remain subject to the ITAR,

even when incorporated into higher order assemblies or end-items. IRFPA, permanent encapsulated sensor assemblies, camera cores, monoculars, binoculars, and other higher order systems not enumerated on the USML are generally subject to the EAR.

Paragraph (d) is revised to move controls on Global Navigation Satellite System (GNSS) equipment from Category XV and to add subparagraphs (1) through (9) to more clearly describe the articles controlled in (d).

Paragraph (d)(1) is added for certain guidance or navigation systems.

Paragraph (d)(2) is added for certain accelerometers.

Paragraph (d)(3) is added for certain gyroscopes or angular rate sensors.

Paragraph (d)(4) is added for certain mobile relative gravimeters.

Paragraph (d)(5) is added for certain mobile gravity gradiometers.

Paragraph (d)(6) is added for Global Navigation Satellite System receiving equipment from Category XV.

Paragraph (d)(7) is added for certain GNSS anti-jam systems employing adaptive antennas.

Paragraph (d)(8) is added for certain GNSS security devices.

Paragraph (d)(9) is added for developmental guidance, navigation, or control devices, systems or equipment funded by the Department of Defense.

Paragraph (e) is revised to add subparagraphs (1) through (15) to more clearly describe the parts and components controlled in (e).

A significant aspect of this more positive, but not yet tiered, proposed USML category is that it does not contain controls on all generic parts, components, accessories, and attachments that are specifically designed or modified for a defense article, regardless of their significance to maintaining a military advantage for the United States. Rather, it contains, with a few exceptions, a positive list of specific types of parts, components, accessories, and attachments that continue to warrant control on the USML. The exceptions pertain to those parts, components, accessories, and attachments identified as “specially designed.”

Paragraph (e)(1) is added for specially designed optical sensors for electronic combat systems controlled in Category XI(a)(4).

Paragraph (e)(2) is added for certain image intensifier tube (IIT) parts and components identified in subparagraphs (i)–(vii).

Paragraph (e)(3) is added for certain wafers incorporating structures for Read-Out Integrated Circuits (ROICs)

controlled in (e)(4) or (e)(5) or for IRFPA detectors controlled in (c)(2).

Paragraph (e)(4) is added for ROICs specially designed for IRFPAs.

Paragraph (e)(5) is added for certain ROICs specially designed for a system, camera core, or packaged IRFPA controlled in paragraph (c).

Paragraph (e)(6) is added for specially designed vacuum packages or other sealed enclosures for an IRFPA or IIT controlled in paragraph (c).

Paragraph (e)(7) is added for integrated IRFPA dewar cooler assembly (IDCA) parts and components identified in subparagraphs (i)–(iv).

Paragraph (e)(8) is added for specially designed IRFPA Joule-Thomson (JT) self-regulating cryostats.

Paragraph (e)(9) is added for specially designed infrared lenses, mirrors, beam splitters or combiners, filters, and treatments and coatings.

Paragraph (e)(10) is added for specially designed drive, control, signal or image processing electronics.

Paragraph (e)(11) is added for signal processing electronics identified in subparagraphs (i)–(iii).

Paragraph (e)(12) is added for specially designed near-to-eye displays.

Paragraph (e)(13) is added for specially designed resonators, receivers, transmitters, modulators, gain media, and drive electronics or frequency converters.

Paragraph (e)(14) is added for two-dimensional infrared scene projector emitter arrays (*i.e.*, resistive arrays) that emit infrared radiation within the 900 nm to 30,000 nm wavelength range.

Paragraph (e)(15) is added for classified parts, components, accessories, attachments, and associated equipment.

A note is added to paragraph (e) to address the incorporation of these defense articles into commercial items.

Paragraph (f) is revised to more clearly describe the technical data and defense services controlled in paragraph (f).

Three notes are added to paragraph (f) to address technical data and defense services when incorporating defense articles into commercial items. Note 1 clarifies that technical data directly related to IITs, IRFPAs, integrated IRFPA dewar cooler assemblies and related wafers and ROICs controlled in this Category remains USML controlled, even when those defense articles are part of a system that is subject to the EAR. Note 2 enumerates certain technical data and software that are directly related to the defense articles controlled in this Category in paragraphs A, B, and C. It also includes a note to paragraph A, identifying

certain technology that is not technical data. Note 3 states that certain technology for the incorporation or integration of IRFPAs and IITs in to items subject to the EAR, including into permanent encapsulated sensor assemblies, is subject to the EAR.

A new (x) paragraph has been added to USML Category XII, allowing ITAR licensing for commodities, software, and technology subject to the EAR provided those commodities, software, and technology are to be used in or with defense articles controlled in USML Category XII *and* are described in the purchase documentation submitted with the application.

Finally, articles common to the Missile Technology Control Regime (MTCR) Annex and the USML are to be identified on the USML with the parenthetical “(MT)” at the end of each section containing such articles. A separate proposed rule will address the sections in the ITAR that include MTCR definitions.

The following definitions explain and amplify terms used in this Category and are provided to assist exporters in understanding the scope of the proposed control.

Charge multiplication is a form of electronic image amplification, the generation of charge carriers as a result of an impact ionization gain process.

Focal plane array is a linear or two-dimensional planar layer, or combination of planar layers, of individual detector elements, with or without readout electronics, which work in the focal plane.

Note: This definition does not include a stack of single detector elements or any two, three, or four element detectors provided time delay and integration is not performed within the element.

Image intensifier tube refers to an imaging device that incorporates a photoemissive transducer (*i.e.*, photocathode) and achieves electron image amplification in the vacuum space.

Microbolometer is a thermal imaging detector that, as a result of a temperature change in the detector caused by the absorption of infrared radiation, is used to generate a usable signal.

Multispectral refers to producing discrete outputs associated with more than one spectral band of response.

Request for Comments

As the U.S. Government works through the proposed revisions to the USML, some control parameters are proposed recognizing that they will control items in normal commercial use

and on the Wassenaar Arrangement’s Dual Use List. With the thought that multiple perspectives would be beneficial to the USML revision process, the Department welcomes the assistance of users of the lists and requests input on the following:

(1) A key goal of this rulemaking is to ensure the USML and the CCL together control all the items that meet Wassenaar Arrangement commitments embodied in Munitions List Categories 5, 11 and 15 (WA–ML15) and the relevant Dual Use List Categories including the IRFPAs in Category 6 (WA–DU 6.A.2). To that end, the public is asked to identify any potential lack of coverage brought about by the proposed rules for Category XII contained in this notice and the new and revised ECCNs published separately by the Department of Commerce when reviewed together.

(2) Another key goal of this rulemaking is to identify items proposed for control on the USML or the CCL that are not controlled on the Wassenaar Arrangement’s Munitions or Dual Use List. The public is asked to identify any items proposed for control on the USML that are not controlled on the Wassenaar Arrangement’s Munitions or Dual Use List.

(3) A third key goal of this rulemaking is to establish a “bright line” between the USML and the CCL for the control of these materials. The public is asked to provide specific examples of control criteria that do not clearly describe items that would be defense articles and thus do not establish a “bright line” between the USML and the CCL.

(4) Although the proposed revisions to the USML do not preclude the possibility that items in normal commercial use would or should be ITAR-controlled because, *e.g.*, they provide the United States with a critical military or intelligence advantage, the U.S. government does not want to inadvertently control items on the ITAR that are in normal commercial use. Items that would be controlled on the USML in this proposed rule have been identified as possessing parameters or characteristics that provide a critical military or intelligence advantage. The public is thus asked to provide specific examples of items, if any, that would be controlled by the revised USML Category XII that are now in normal commercial use. The examples should demonstrate actual commercial use, not just potential or theoretical use, with supporting documents, as well as foreign availability of such items.

(5) For any criteria the public believes control items in normal commercial use, the public is asked to identify parameters or characteristics that cover

items exclusively or primarily in military use.

(6) For any criteria the public believes control items in normal commercial use, the public is asked to identify the multilateral controls (such as the Wassenaar Arrangement's Dual Use List), if any, for such items, and the consequences of such items being controlled on the USML.

(7) DDTC seeks public comments on each paragraph of the proposed USML Category XII. In addition, DDTC specifically seeks public comments on the following concepts that are introduced in proposed USML Category XII: A) Using integration of an IRFPA into a permanent encapsulated sensor assembly as a control parameter; B) using the incorporation of an IRFPA into an infrared imaging camera core as a control parameter and the definition of camera cores in the note to XII(c)(12); C) the weapon shock load control criterion in XII(c)(12)(ii); and D) proposed controls on specific technical data in XII(f).

Regulatory Analysis and Notices

Administrative Procedure Act

The Department of State is of the opinion that controlling the import and export of defense articles and services is a foreign affairs function of the United States Government and that rules implementing this function are exempt from sections 553 (rulemaking) and 554 (adjudications) of the Administrative Procedure Act (APA). Although the Department is of the opinion that this rule is exempt from the rulemaking provisions of the APA, the Department is publishing this rule with a 60-day provision for public comment and without prejudice to its determination that controlling the import and export of defense services is a foreign affairs function.

Regulatory Flexibility Act

Since this rule is exempt from the rulemaking provisions of 5 U.S.C. 553, it does not require analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This proposed amendment does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

This proposed amendment has been found not to be a major rule within the meaning of the Small Business Regulatory Enforcement Fairness Act of 1996.

Executive Orders 12372 and 13132

This proposed amendment will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this proposed amendment does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this proposed amendment.

Executive Orders 12866 and 13563

Executive Orders 13563 and 12866 direct agencies to assess costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget (OMB).

Executive Order 12988

The Department of State has reviewed the proposed amendment in light of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department of State has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, Executive Order 13175 does not apply to this rulemaking.

Paperwork Reduction Act

Following is a listing of approved Department of State collections that will be affected by revision of the U.S. Munitions List (USML) and the Commerce Control List pursuant to the President's Export Control Reform (ECR) initiative. The list of collections and the description of the manner in which they will be affected pertains to revision of the USML in its entirety, not only to the categories published in this rule. In accordance with the Paperwork Reduction Act, the Department of State will request comment on these collections from all interested persons at the appropriate time. In particular, the Department will seek comment on changes to licensing burden based on implementation of regulatory changes pursuant to ECR, and on projected changes based on continued implementation of regulatory changes pursuant to ECR. The information collections are as follows:

(1) Statement of Registration, DS-2032, OMB No. 1405-0002. The Department estimates that between 3,000 and 5,000 of the currently-registered persons will not need to maintain registration following full revision of the USML. This would result in a burden reduction of between 6,000 and 10,000 hours annually, based on a revised time burden of two hours to complete a Statement of Registration.

(2) Application/License for Permanent Export of Unclassified Defense Articles and Related Unclassified Technical Data, DSP-5, OMB No. 1405-0003. The Department estimates that there will be 35,000 fewer DSP-5 submissions annually following full revision of the USML. This would result in a burden reduction of 35,000 hours annually.

(3) Application/License for Temporary Import of Unclassified Defense Articles, DSP-61, OMB No. 1405-0013. The Department estimates that there will be 200 fewer DSP-61 submissions annually following full revision of the USML. This would result in a burden reduction of 100 hours annually.

(4) Application/License for Temporary Export of Unclassified Defense Articles, DSP-73, OMB No. 1405-0023. The Department estimates that there will be 800 fewer DSP-73 submissions annually following full revision of the USML. This would result in a burden reduction of 800 hours annually.

(5) Application for Amendment to License for Export or Import of Classified or Unclassified Defense Articles and Related Technical Data, DSP-6, -62, -74, -119, OMB No. 1405-

0092. The Department estimates that there will be 2,000 fewer amendment submissions annually following full revision of the USML. This would result in a burden reduction of 1,000 hours annually.

(6) Request for Approval of Manufacturing License Agreements, Technical Assistance Agreements, and Other Agreements, DSP-5, OMB No. 1405-0093. The Department estimates that there will be 1,000 fewer agreement submissions annually following full revision of the USML. This would result in a burden reduction of 2,000 hours annually.

(7) Maintenance of Records by Registrants, OMB No. 1405-0111. The requirement to actively maintain records pursuant to provisions of the ITAR will decline commensurate with the drop in the number of persons who will be required to register with the Department pursuant to the ITAR. As stated above, the Department estimates that up to 5,000 of the currently-registered persons will not need to maintain registration following full revision of the USML. This would result in a burden reduction of 100,000 hours annually. However, the ITAR does provide for the maintenance of records for a period of five years. Therefore, persons newly relieved of the requirement to register with the Department may still be required to maintain records.

List of Subjects in 22 CFR Part 121

Arms and munitions, Exports.

Accordingly, for the reasons set forth above, title 22, chapter I, subchapter M, part 121 is proposed to be amended as follows:

PART 121—THE UNITED STATES MUNITIONS LIST

■ 1. The authority citation for part 121 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90-629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; Pub. L. 105-261, 112 Stat. 1920; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

§ 121.1 [Amended]

■ 2. Section 121.1 is amended by removing and reserving paragraph (e) in U.S. Munitions List Category VIII.

■ 3. Section 121.1 is amended by revising U.S. Munitions List Category XII to read as follows:

§ 121.1 The United States Munitions List.

* * * * *

Category XII—Fire Control, Range Finder, Optical and Guidance and Control Equipment

*(a) Fire control, weapons sights, aiming, and imaging systems and equipment, as follows:

(1) Fire control systems or equipment, and specially designed parts and components therefor;

(2) Weapon sights, weapon aiming systems or equipment, and weapon imaging systems or equipment (*e.g.*, clip-on), with or without an integrated viewer, display, or reticle, and incorporating or specially designed to incorporate any of the following:

(i) An infrared focal plane array having a peak response at a wavelength exceeding 1,000 nm;

(ii) An article subject to this subchapter; or

(iii) A ballistic computer for adjusting the aim point display;

(3) Electronic or optical weapon positioning, laying, or spotting systems or equipment;

(4) Laser spot trackers or laser spot detection, location or imaging systems or equipment, with an operational wavelength shorter than 400 nm or longer than 710 nm, and a detection range greater than 300 m;

Note to paragraph (a)(4): For controls on LIDAR, see paragraph (b)(9) of this category.

(5) Bomb sights or bombing computers;

(6) Electro-optical missile or ordnance tracking systems or equipment, or electro-optical ordnance guidance systems or equipment;

(7) Electro-optical systems or equipment that automatically detect and locate weapons launch or fire;

(8) Remote wind-sensing systems or equipment specially designed for ballistic-corrected aiming, and specially designed parts and components therefor;

(9) Helmet mounted display (HMD) systems or equipment, incorporating optical sights or slewing devices, which include the ability to aim, launch, track, or manage munitions, or control infrared imaging systems or equipment, other than such items controlled in Category VIII, (*e.g.*, Combat Vehicle Crew HMD, Mounted Warrior HMD, Integrated Helmet Assembly Subsystem, Drivers Head Tracked Vision System).

*(b) Lasers, and laser systems and equipment, as follows:

(1) Laser target designators or coded target markers;

(2) Aiming or target illumination systems or equipment having a laser output wavelength exceeding 710 nm;

(3) Laser rangefinders having any of the following:

(i) Q-switched laser pulse; or

(ii) Laser output wavelength exceeding 1,000 nm;

(4) Targeting or target location systems or equipment incorporating or specially designed to incorporate a laser rangefinder controlled in paragraph (b)(3) of this category, and incorporating or specially designed to incorporate a Global Navigation Satellite System (GNSS), guidance or navigation article controlled in paragraph (d) of this category (MT if designed or modified for rockets, missiles, SLVs, drones, or unmanned aerial vehicle systems capable of delivering at least a 500 kg payload to a range of at least 300 km range);

(5) Systems or equipment that use laser energy with an output wavelength exceeding 710 nm to exploit differential target-background retroreflectance in order to detect personnel or optical/electro-optical equipment (*e.g.*, optical augmentation systems);

(6) Light detection and ranging (LIDAR), laser detection and ranging (LADAR), or range-gated systems or equipment, incorporating or specially designed to incorporate an article controlled in this subchapter (MT if designed or modified for rockets, missiles, SLVs, drones, or unmanned aerial vehicle systems capable of delivering at least a 500 kg payload to a range of at least 300 km);

Note to paragraph (b)(6): This paragraph does not control LIDAR systems or equipment for civil automotive applications having a range limited to 200 m or less.

(7) Synthetic aperture LIDAR or LADAR systems or equipment, having a stand-off range of 100 m or greater (MT if designed or modified for rockets, missiles, SLVs, drones, or unmanned aerial vehicle systems capable of delivering at least a 500 kg payload to a range of at least 300 km);

(8) LIDAR, LADAR, or other laser range-gated systems or equipment, as follows (MT if designed or modified for rockets, missiles, SLVs, drones, or unmanned aerial vehicle systems capable of delivering at least a 500 kg payload to a range of at least 300 km):

(i) Systems or equipment having a resolution (*i.e.*, ground point spacing) of 0.2 m or less (better) from an altitude above ground level of greater than 16,500 ft, and incorporating or specially designed to incorporate a gimbal-mounted transmitter or beam director, and specially designed parts and components therefor;

(ii) Aircraft systems or equipment having a laser output wavelength exceeding 1,000 nm and a detection range exceeding 500 m for an obstacle

with a diameter or width less than or equal to 10 mm (e.g., wire, power line);

(iii) Systems or equipment having an electrical bandwidth of 100 MHz or greater, and incorporating or specially designed to incorporate either a Geiger-mode detector array having at least 32 elements or a linear-mode detector array having at least 128 elements;

(iv) Systems or equipment employing coherent heterodyne or coherent homodyne detection techniques, having an angular resolution of less (better) than 100 microradians and an operational carrier noise ratio (CNR) less than 10;

(v) Systems or equipment that automatically classify or identify submersibles, mines, unexploded ordnance or improvised explosive devices (IEDs); or

(vi) Systems or equipment specially designed for obstacle avoidance or autonomous navigation in ground vehicles controlled in Category VII;

Note to paragraphs (b)(4) and (b)(6) through (8): "Payload" is the total mass that can be carried or delivered by the specified rocket, missile, SLV, drone or unmanned aerial vehicle that is not used to maintain flight. For definition of "range" as it pertains to rocket systems, see note 1 to paragraph (a) of USML Category IV. For definition of "range" as it pertains to aircraft systems, see note to paragraph (a) of USML Category VIII.

(9) Lasers operating at a wavelength exceeding 3,000 nm that provide a modulated output for systems or equipment controlled in Category XI(a)(4);

(10) Tunable semiconductor lasers having an output wavelength exceeding 1,400 nm and an output power greater than 1 W;

(11) Non-tunable single transverse mode semiconductor lasers having an output wavelength exceeding 1,510 nm and either an average output power or continuous wave (CW) output power greater than 2 W;

(12) Non-tunable multiple transverse mode semiconductor lasers having an output wavelength exceeding 1,900 nm and either an average output power or CW output power greater than 2 W;

(13) Laser stacked arrays as follows:

(i) Having an output wavelength not exceeding 1,400 nm and a peak pulsed power density greater than 3,300 W/cm²;

(ii) Having an output wavelength exceeding 1,400 nm but less than 1,900 nm and a peak pulsed power density greater than 700 W/cm²;

(iii) Having an output wavelength exceeding 1,900 nm and a peak pulsed power density greater than 70 W/cm²; or

(iv) Having an output wavelength exceeding 1,900 nm, and either an

average output power or CW output power greater than 20W;

(14) Developmental lasers and laser systems or equipment funded by the Department of Defense;

Note 1 to paragraph (b)(14): This paragraph does not control developmental lasers and laser systems or equipment (a) in production, (b) determined to be subject to the EAR via a commodity jurisdiction determination (see § 120.4 of this subchapter), or (c) identified in the relevant Department of Defense contract or other funding authorization as being developed for both civil and military applications.

Note 2 to paragraph (b)(14): Note 1 does not apply to defense articles enumerated on the U.S. Munitions List, whether in production or development.

Note 3 to paragraph (b)(14): This provision is applicable to those contracts or other funding authorizations that are dated XXXX, 2016, or later.

*(c) Infrared focal plane arrays, image intensifier tubes, night vision, electro-optic, infrared and terahertz systems, equipment and accessories, including cameras and cores, as follows:

(1) Image intensifier tubes (IITs) having a peak response within the wavelength range exceeding 400 nm but not exceeding 2,050 nm and incorporating either a microchannel plate described in paragraph (e)(2)(i) of this category or electron sensing device described in paragraph (e)(2)(iv) of this category, as follows, and specially designed parts and components therefor:

(i) Incorporating a multialkali photocathode having a luminous sensitivity exceeding 500 microamps per lumen (e.g., GEN 2 IITs);

(ii) Incorporating a compound semiconductor photocathode having a radiant sensitivity exceeding 20 mA/W (e.g., GEN 3 IITs);

(2) Photon detector, microbolometer detector, or multispectral detector infrared focal plane arrays (IRFPAs) having a peak response within the wavelength range exceeding 900 nm but not exceeding 30,000 nm and not integrated into a permanent encapsulated sensor assembly, and detector elements therefor;

Note 1 to paragraph (c)(2): This paragraph does not control lead sulfide or lead selenide IRFPAs having a peak response within the wavelength range exceeding 1,000 nm but not exceeding 5,000 nm and not exceeding 16 detector elements, or pyroelectric IRFPAs with detectors composed of any of the following or their variants: Triglycine sulphate, lead-lanthanum-zirconium titanate, lithium tantalite, polyvinylidene fluoride, or strontium barium niobate.

Note 2 to paragraph (c)(2): For controls on readout integrated circuits (ROICs), see paragraphs (e)(4) and (e)(5) of this category.

(3) One-dimensional photon detector IRFPAs described in paragraph (c)(2) of this category in a permanent encapsulated sensor assembly, having greater than 640 detector elements;

(4) Two-dimensional photon detector IRFPAs described in paragraph (c)(2) of this category in a permanent encapsulated sensor assembly, having greater than 256 detector elements;

(5) Microbolometer IRFPAs described in paragraph (c)(2) of this category in a permanent encapsulated sensor assembly, having greater than 328,000 detector elements;

(6) Multispectral IRFPAs in a permanent encapsulated sensor assembly, having a peak response in any spectral band within the wavelength range exceeding 1,500 nm but not exceeding 30,000 nm;

(7) Charge multiplication focal plane arrays having greater than 1,600 elements in any dimension and having a maximum radiant sensitivity exceeding 50 mA/W for any wavelength exceeding 760 nm but not exceeding 900 nm, and avalanche detector elements therefor;

(8) Charge multiplication focal plane arrays described in paragraph (c)(7) of this category in a permanent encapsulated sensor assembly, and avalanche detector elements therefor;

(9) Integrated IRFPA dewar cooler assemblies (IDCAs), with or without an IRFPA, having any of the following:

(i) Cryocoolers having a cooling source temperature below 218 K and a mean-time-to-failure (MTTF) in excess of 3000 hours;

(ii) Active cold fingers;

(iii) Variable or dual aperture mechanisms; or

(iv) Dewars specially designed for articles controlled in paragraphs (a), (b), or (c) of this category;

(10) Gimbals with two or more axes of active stabilization having a minimum root-mean-square (RMS) stabilization better (less) than 200 microradians, and specially designed for articles controlled in this subchapter;

(11) Gimbals with two or more axes of active stabilization having a minimum root-mean-square (RMS) stabilization better (less) than 100 microradians;

Note to paragraph (c)(11): This paragraph does not control gimbals containing only a non-removable camera payload operating exclusively in the visible spectrum (i.e., 400 nm to 760 nm).

(12) Infrared imaging camera cores (e.g., modules, engines, kits), and specially designed electronics and

optics therefor, having any of the following:

(i) An image intensifier tube described in paragraph (c)(1) of this category;

(ii) Output imagery when subject to more than 20 weapon shock load events of 325 g for 0.4 ms and a microbolometer IRFPA having greater than 111,000 detector elements;

(iii) A microbolometer IRFPA described in paragraph (c)(2) of this category having greater than 328,000 detector elements, or a microbolometer IRFPA described in paragraph (c)(5) of this category;

(iv) An IDCA described in paragraph (c)(9) of this category, or IDCA parts or components described in paragraph (e)(7) of this category;

(v) A one-dimensional photon detector IRFPA described in paragraph (c)(2) of this category having a peak response within the wavelength range exceeding 900 nm but not exceeding 2,500 nm and greater than 640 detector elements;

(vi) A one-dimensional or two-dimensional photon detector IRFPA described in paragraph (c)(2) of this category having a peak response within the wavelength range exceeding 2,500 nm but not exceeding 30,000 nm and greater than 256 detector elements;

(vii) A one-dimensional photon detector IRFPA described in paragraph (c)(3) of this category;

(viii) A two-dimensional photon detector IRFPA described in paragraph (c)(2) or (4) of this category having a peak response within the wavelength range exceeding 900 nm but not exceeding 2,500 nm, and greater than 111,000 detector elements;

(ix) A two-dimensional photon detector IRFPA described in paragraph (c)(4) of this category having a peak response within the wavelength range exceeding 2,500 nm but not exceeding 30,000 nm;

(x) A multispectral infrared focal plane array described in paragraph (c)(2) or (6) of this category; or

(xi) A charge multiplication IRFPA controlled in paragraph (c)(7) or (8) of this category;

Note to paragraph (c)(12): The articles controlled by this paragraph have sufficient electronics to enable as a minimum the output of an analog or digital signal once power is applied.

(13) Binoculars, bioculars, monoculars, goggles, or head or helmet-mounted imaging systems or equipment (including video-based articles having a separate near-to-eye display) that incorporate or are specially designed to incorporate any of the following, and specially designed electronics, optics, and displays therefor:

(i) An IIT controlled in this category; or

(ii) An infrared imaging camera core controlled in paragraph (c)(12)(i) through (xi) of this category;

Note to paragraph(c)(13): The articles controlled in this paragraph include binoculars, bioculars, monoculars, goggles, or head- or helmet-mounted imaging systems or equipment (including video-based articles having a separate near-to-eye display) that incorporate or are specially designed to incorporate an IRFPA or IIT article (*e.g.*, IDCA, IRFPA assembly) and electronics separately.

(14) Targeting systems or equipment incorporating or specially designed to incorporate an article controlled in this category (*e.g.*, pods, IBAS, SGFLIR, gunner TIS), and specially designed parts and components therefor;

(15) Infrared search and track (IRST) systems or equipment that incorporate or are specially designed to incorporate an article controlled in this category, and maintain positional or angular state of a target through time, and specially designed parts and components therefor;

(16) Infrared imaging systems or equipment (*e.g.*, fully packaged cameras) incorporating or specially designed to incorporate an article controlled in this category, as follows, and specially designed electronics, optics, and displays therefor:

(i) Having two or more axes of active stabilization and a minimum root-mean-square (RMS) stabilization better (less) than 200 microradians;

(ii) Mobile reconnaissance, scout, or surveillance systems or equipment providing real-time target location at ranges greater than 5 km (*e.g.*, LRAS, CIV, HTI, SeeSpot, MMS);

(iii) Fixed-site reconnaissance, surveillance or perimeter security systems or equipment having greater than 640 detector elements in any dimension;

(iv) Combat vehicle, tactical wheeled vehicle, naval vessel, or aircraft pilotage systems or equipment having a variable field of view or field of regard (*e.g.*, electronic pan or tilt), and either an IRFPA article controlled in this subchapter with greater than 640 detector elements in any dimension, or an IIT controlled in this category (*e.g.*, DAS, DVE, SeaFLIR, PNVs);

Note to paragraph (c)(16)(iv): This paragraph does not control distributed aperture sensors specially designed for civil automotive lane departure warning or collision avoidance.

(v) Multispectral imaging systems or equipment that either incorporate a multispectral IRFPA described in paragraph (c)(2) or (6) of this category,

or classify or identify military or intelligence targets or characteristics;

(vi) Automated missile detection or warning;

(vii) Hardened to withstand electromagnetic pulse (EMP) or chemical, biological, or radiological threats;

(viii) Incorporating mechanism(s) to reduce signature; or

(ix) Specially designed for military platforms controlled in USML Categories VI, VII or VIII (MT if designed or modified for unmanned aerial vehicle systems capable of delivering at least a 500 kg payload to a range of at least 300 km);

(17) Terahertz imaging systems or equipment having a peak response in the frequency range exceeding 30 GHz but not exceeding 3000 GHz and having a resolution less (better) than 0.5 milliradians at a standoff range of 100 m;

(18) Near-to-eye display systems or equipment, specially designed for articles controlled in this subchapter;

(19) Systems or equipment that project radiometrically calibrated scenes directly into the entrance aperture of an electro-optical or infrared (EO/IR) sensor controlled in this subchapter within either the spectral band exceeding 10 nm but not exceeding 400 nm, or the spectral band exceeding 900 nm but not exceeding 30,000 nm; or

(20) Systems or equipment incorporating an infrared (IR) beacon or emitter specially designed for Identification Friend or Foe (IFF), and specially designed parts and components therefor;

(21) Developmental imaging systems or equipment funded by the Department of Defense.

Note 1 to paragraph (c)(21): This paragraph does not control imaging systems or equipment (a) in production; (b) determined to be subject to the EAR via a commodity jurisdiction determination (see § 120.4 of this subchapter), or (c) identified in the relevant Department of Defense contract or other funding authorization as being developed for both civil and military applications.

Note 2 to paragraph (c)(21): Note 1 does not apply to defense articles enumerated on the U.S. Munitions List, whether in production or development.

Note 3 to paragraph (c)(21): This provision is applicable to those contracts or other funding authorizations that are dated XXXX, 2016, or later.

Note 1 to paragraph (c): A permanent encapsulated sensor assembly (*e.g.*, sealed enclosure, vacuum package) prevents direct access to the IRFPA, disassembly of the sensor assembly, and removal of the IRFPA without destruction or damage to the IRFPA.

Note 2 to paragraph (c): The articles described in paragraphs (c)(1) through (5), (c)(7), (c)(8), and (c)(12) other than (c)(12)(ix) having greater than 640 detector elements in any dimension, and (c)(12)(x) are subject to the EAR when, prior to export, reexport, retransfer, or temporary import, they are integrated into and included as an integral part of an item subject to the EAR, and cannot be removed without destruction or damage to the article or render the item inoperable. Articles are not subject to the EAR until integrated into the item subject to the EAR. Defense articles intended to be integrated, and technical data and defense services directly related thereto remain subject to the ITAR prior to integration. See paragraph (f) of this category for enumerated technical data and software, and specific information subject to the EAR.

(d) Guidance, navigation, and control systems and equipment as follows:

(1) Guidance or navigation systems (e.g., inertial navigation systems, inertial measurement units, inertial reference units, attitude and heading reference systems) as follows (MT if designed or modified for rockets, missiles, SLVs, drones, or unmanned aerial vehicle systems capable of a range greater than or equal to 300 km);

(i) Having a circle of equal probability (CEP) of position error rate less (better) than 0.35 nautical miles per hour;

(ii) Having a heading error or true north determination of less (better) than 0.50 mrad secant (latitude) (0.02865 degrees secant (latitude)); or

(iii) Specified to function at linear acceleration levels exceeding 25 g;

Note to paragraph (d)(1): For aircraft and unmanned aerial vehicle guidance or navigation systems, see USML Category VIII(e). For rocket or missile flight control and guidance systems (including guidance sets), see USML Category IV(h).

(2) Accelerometers having a bias stability of less (better) than 20 μ g, a scale factor stability of less (better) than 20 parts per million, or capable of measuring greater than 100,000 g (MT if having a scale factor repeatability less (better) than 1250 ppm and bias repeatability less (better) than 1250 micro g or specified to function at acceleration levels greater than 100 g);

Note 1 to paragraph (d)(2): For weapon fuze accelerometers, see USML Category III(d) or IV(h).

Note 2 to paragraph (d)(2): MT designation does not include accelerometers that are designed to measure vibration or shock.

(3) Gyroscopes or angular rate sensors having an angle random walk of less (better) than 0.00125 degree per square root hour or having a bias stability less (better) than 0.0015 degrees per hour (MT if having a rated drift stability of less than 0.5 degrees (1 sigma or rms)

per hour in a 1 g environment or specified to function at acceleration levels greater than 100 g);

(4) Mobile relative gravimeters, having automatic motion compensation, with an in-service accuracy of less (better) than 0.4 mGal (MT if designed or modified for airborne or marine use and having a time to steady-state registration of two minutes or less);

(5) Mobile gravity gradiometers having an accuracy of less (better) than 10 Eötvös squared per radian per second for any component of the gravity gradient tensor, and having a spatial gravity wavelength resolution of 50 m or less (MT if designed or modified for airborne or marine use);

Note to paragraph (d)(5): “Eötvös” is a unit of acceleration divided by distance that was used in conjunction with the older centimeter-gram-second system of units. The Eötvös is defined as 1/1,000,000,000 Galileo (Gal) per centimeter.

(6) Global Navigation Satellite System (GNSS) receiving equipment, as follows, and specially designed parts and components therefor:

(i) Global Navigation Satellite System (GNSS) receiving equipment specially designed for military applications (MT if designed or modified for airborne applications and capable of providing navigation information at speeds in excess of 600 m/s);

(ii) Global Positioning System (GPS) receiving equipment specially designed for encryption or decryption (e.g., Y-Code, M-Code) of GPS precise positioning service (PPS) signals (MT if designed or modified for airborne applications);

(iii) GPS receiving equipment specially designed for use with a null steering antenna, an electronically steerable antenna, or including a null steering antenna designed to reduce or avoid jamming signals (MT if designed or modified for airborne applications); or

Note to paragraph (6)(iii): The articles described in this paragraph are subject to the EAR when, prior to export, reexport, retransfer, or temporary import, they are integrated into and included as an integral part of an item subject to the EAR. Articles do not become subject to the EAR until integrated into the item subject to the EAR. Export, reexport, retransfer, or temporary import of, and technical data and defense services directly related to, defense articles intended to be integrated, remain subject to the ITAR.

(iv) GPS receiving equipment specially designed for use with rockets, missiles, space launch vehicles (SLVs), drones, or unmanned air vehicle systems capable of delivering at least a

500 kg payload to a range of at least 300 km (MT);

Note to paragraph (6)(iv): “Payload” is the total mass that can be carried or delivered by the specified rocket, missile, SLV, drone or unmanned aerial vehicle that is not used to maintain flight. For definition of “range” as it pertains to rocket systems, see note 1 to paragraph (a) of USML Category IV. For definition of “range” as it pertains to aircraft systems, see note to paragraph (a) of USML Category VIII.

(7) GNSS anti-jam systems employing adaptive antennas that have a minimum of four antenna elements, add 35 dB or greater anti-jam margin, and produce nulls in the direction of jammers or high-gain beams in the direction of satellites at any ranging code frequency;

(8) GNSS security devices (e.g., Selective Availability Anti-Spoofing Modules, Security Modules, and Auxiliary Output Chips), Selective Availability Anti-Spoofing Module (SAASM), Security Module (SM) and Auxiliary Output Chip (AOC) chips; or

(9) Developmental guidance, navigation, or control devices, systems or equipment funded by the Department of Defense (MT if designed or modified for rockets, missiles, SLVs, drones, or unmanned aerial vehicle systems capable of a range equal to or greater than 300 km);

Note 1 to paragraph (d)(9): This paragraph does not control guidance, navigation, or control, systems, or equipment (a) in production, (b) determined to be subject to the EAR via a commodity jurisdiction determination (see § 120.4 of this subchapter), or (c) identified in the relevant Department of Defense contract or other funding authorization as being developed for both civil and military applications.

Note 2 to paragraph (d)(9): Note 1 does not apply to defense articles enumerated on the U.S. Munitions List, whether in production or development.

Note 3 to paragraph (d)(9): This provision is applicable to those contracts or other funding authorizations that are dated XXXX, 2016, or later.

Note 4 to paragraph (d)(9): For definition of “range” as it pertains to rocket systems, see note 1 to paragraph (a) of USML Category IV. For definition of “range” as it pertains to aircraft systems, see note to paragraph (a) of USML Category VIII.

(e) Parts, components, accessories, attachments, and associated equipment as follows:

(1) Optical sensors having a spectral filter for systems or equipment controlled in USML Category XI(a)(4), or optical sensor assemblies that provide threat warning or tracking for systems or equipment controlled in Category

XI(a)(4) and specially designed optics and electronics therefor;

(2) Image intensifier tube (IIT) parts and components as follows:

(i) Microchannel plates having a hole pitch (center-to-center spacing) of 12 μm or less;

(ii) Multialkali photocathodes (*e.g.*, S-20 and S-25) having a luminous sensitivity exceeding 500 microamps per lumen;

(iii) III/V compound semiconductor (*e.g.*, GaAs or GaInAs) photocathodes and transferred electron photocathodes having a radiant sensitivity exceeding 20 mA/W;

(iv) Electron sensing devices with detectors having a non-binned center-to-center spacing less than 100 μm , and either achieving charge multiplication within the vacuum space other than by a microchannel plate or specially designed for operation with a microchannel plate;

(v) Phosphor screens, including output faceplates, specially designed for IITs controlled in this category;

(vi) Miniature autogated power supplies providing internal sensing and control of the photocathode to increase the dynamic range of IITs controlled in this category; or

(vii) Fiber-optic inverters, couplers or tapers specially designed for IITs controlled in this category;

(3) Wafers incorporating structures for either a ROIC controlled in paragraph (e)(4) or (5) of this category, or an IRFPA or detector elements therefor controlled in paragraph (c)(2) of this category;

(4) Read-Out Integrated Circuits (ROICs) specially designed for an IRFPA controlled in paragraph (c)(2) of this category or detector elements therefor, as follows:

(i) One-dimensional photon detector IRFPA having greater than 640 detector elements;

(ii) Two-dimensional photon detector IRFPA having greater than 256 detector elements;

(iii) A microbolometer IRFPA having greater than 19,200 elements; or

(iv) Multispectral IRFPA;

Note to paragraph (e)(4): ROICs are specially designed for an infrared focal plane array detector even if the detector is incorporated into an item that is not enumerated on the U.S. Munitions List.

(5) ROICs specially designed for a camera/core/package IRFPA subject to the controls of this subchapter;

(6) Vacuum packages or other sealed enclosures for an IRFPA or IIT controlled in paragraph (c) of this category specially designed for incorporation or integration into an article controlled in paragraphs (a), (b), or (c) of this category;

(7) Integrated IRFPA dewar cooler assembly (IDCA) parts and components, as follows:

(i) Cryocoolers having a cooling source temperature below 218 K and a mean-time-to-failure (MTTF) in excess of 3000 hours;

(ii) Active cold fingers;

(iii) Variable or dual aperture mechanisms; or

(iv) Dewars specially designed for articles controlled in paragraphs (a), (b) or (c) of this category;

(8) IRFPA Joule-Thomson (JT) self-regulating cryostats specially designed for articles controlled in this subchapter;

(9) Infrared lenses, mirrors, beam splitters or combiners, filters, and treatments and coatings, specially designed for any article controlled in this category;

(10) Drive, control, signal or image processing electronics, specially designed for articles controlled in this category;

(11) Signal processing electronics, attachments or accessories that provide:

(i) Automatic or aided detection and recognition, classification, identification or discrimination of military or intelligence items;

(ii) Multi-sensor fusion other than image blending; or

Note to paragraph (e)(11)(ii): Multi-sensor fusion refers to automatically combining imagery or information from two or more sensors, including at least one article controlled in this category, to improve classification, identification, or tracking of targets relative to any of the individual sensors.

(iii) Target aim point adjustment;

(12) Near-to-eye displays specially designed for articles controlled in this category;

(13) Resonators, receivers, transmitters, modulators, gain media, and drive electronics or frequency converters specially designed for laser systems or equipment controlled in this category;

(14) Two-dimensional infrared scene projector emitter arrays (*i.e.*, resistive arrays) that emit infrared radiation within the 900 nm to 30,000 nm wavelength range; or

(15) Any part, component, accessory, attachment, or associated equipment, that:

(i) Is "classified";

(ii) Contains "classified" software;

(iii) Is manufactured using "classified" production data; or

(iv) Is being developed using "classified" information.

Note to paragraph (e)(15): "Classified" means classified pursuant to Executive Order

13526, or predecessor order, and a security classification guide developed pursuant thereto or equivalent, or to the corresponding classification rules of another government.

Note to paragraph (e): The articles described in this paragraph are subject to the EAR when, prior to export, reexport, retransfer, or temporary import, they are integrated into and included as an integral part of an item subject to the EAR, and cannot be removed without destruction or damage to the article or render the item inoperable. Articles are not subject to the EAR until integrated into the item subject to the EAR. Defense articles intended to be integrated, and technical data and defense services directly related thereto, remain subject to the ITAR prior to integration. See paragraph (f) of this category for enumerated technical data and software, and specific information subject to the EAR.

*** (f) Technical data** (as defined in § 120.10 of this subchapter) and defense services (as defined in § 120.9 of this subchapter) directly related to the defense articles enumerated in paragraphs (a) through (e) of this category. (See § 125.4 of this subchapter for exemptions.) (MT for technical data and defense services related to articles designated as such.)

Note 1 to paragraph (f): Technical data and defense services directly related to image intensifier tubes and specially designed parts and components therefor controlled in paragraph (c)(1) of this category, infrared focal plane arrays (IRFPAs) and detector elements therefor controlled in paragraph (c)(2) of this category, integrated IRFPA dewar cooler assemblies (IDCAs) controlled in paragraph (c)(9) of this category, wafers incorporating IRFPA or ROIC structures controlled in paragraph (e)(3) of this category, and specially designed readout integrated circuits (ROICs) controlled in paragraphs (e)(4) and (5) of this category, remain subject to the ITAR even if the technical data or defense services could also apply to items subject to the EAR.

Note 2 to paragraph (f): Software and technical data include:

A. Design or manufacturing process descriptions (*e.g.*, steps, sequences, conditions, parameters) for lasers described in paragraphs (b)(6) and (b)(9) through (13) of this category, IITs controlled in paragraph (c)(1) of this category and their parts and components controlled in paragraph (e)(2) of this category (including tube sealing techniques, interface techniques within the vacuum space for photocathodes, microchannel plates, phosphor screens, input glass-window faceplates, input or output fiber optics (*e.g.*, inverter)), IRFPAs and detector elements therefor controlled in paragraph (c)(2) of this category, integrated IRFPA dewar cooler assemblies (IDCAs) controlled in paragraph (c)(9) of this category, wafers incorporating structures for an IRFPA and detector elements therefor controlled in paragraph (c)(2) or structures for ROICs controlled in paragraph (e)(4) or (5)

of this category, and specially designed ROICs controlled in paragraphs (e)(4) and (5) of this category (including bonding or mating (e.g., hybridization of IRFPA detectors and ROICs), prediction or optimization of IRFPAs or ROICs at cryogenic temperatures, junction formation, passivation).

Note to paragraph A of note 2 to paragraph (f): Technical data does not include information directly related to basic operating instructions, testing results, incorporating or integrating IRFPAs into higher level packaged assemblies not enumerated in this category, or external interface control documentation associated with such assemblies or assemblies subject to the EAR, provided such information does not include design methodology, engineering analysis, or manufacturing know-how for a USML controlled IRFPA.

B. Software that converts an article controlled in this category into an item subject to the EAR or an item subject to the EAR into an article controlled in this category is directly related to the defense article controlled in this category. When a defense article has

been converted into an item subject to the EAR through software, the presence of the software that prevents the item from meeting or exceeding a USML control parameter does not make the item subject to the ITAR.

C. EO/IR simulation or projection system software that replicates via simulation either the output data or information provided by any article controlled in this category, a radiometrically calibrated spectral signature of any article controlled in this subchapter, volumetric effects of plumes or military operational obscurants, or countermeasure effects.

Note 3 to paragraph (f): Technology for incorporating or integrating IRFPAs into permanent encapsulated sensor assemblies subject to the EAR, or integrating such assemblies into an item subject to the EAR, and integrating IITs into an item subject to the EAR, including integrating items subject to the EAR into foreign military commodities outside the United States, is subject to the EAR.

(g)–(w) [Reserved]

(x) Commodities, software, and technology subject to the EAR (see § 120.42 of this subchapter) used in or with defense articles controlled in this category.

Note to paragraph (x): Use of this paragraph is limited to license applications for defense articles controlled in this category where the purchase documentation includes commodities, software, or technology subject to the EAR (see § 123.1(b) of this subchapter).

* * * * *

§ 121.1 [Amended]

■ 4. Section 121.1 is amended by removing and reserving paragraph (c) in U.S. Munitions List Category XV.

Rose E. Gottemoeller,
Under Secretary, Arms Control and International Security, Department of State.
[FR Doc. 2015–09673 Filed 5–4–15; 8:45 am]
BILLING CODE 4710–25–P

SBU/DRAFT

Temporary Modification of Category I of the United States Munitions List

Consistent with the International Traffic in Arms Regulations (ITAR), 22 C.F.R. § 126.2, the Acting Deputy Assistant Secretary for Defense Trade Controls has determined that it is in the interest of the security and foreign policy of the United States to temporarily modify United States Munitions List (USML) Category I to exclude the following technical data identified in the Settlement Agreement for the matter of *Defense Distributed, et al., v. U.S. Department of State, et al*, Case No. 15-cv-372-RP (W.D. Tex.) (hereinafter “*Defense Distributed*”):

- “Published Files,” i.e., the files described in paragraph 25 of the Second Amended Complaint in *Defense Distributed*.
- “Ghost Gunner Files,” i.e., the files described in paragraph 36 of the Second Amended Complaint in *Defense Distributed*.
- “CAD Files,” i.e., the files described in paragraph 40 of the Second Amended Complaint in *Defense Distributed*.
- “Other Files,” i.e., the files described in paragraphs 44-45 of the Second Amended Complaint in *Defense Distributed*, insofar as those files regard items exclusively: (a) in Category I(a) of the USML, as well as barrels and receivers covered by Category I(g) of the USML that are components of such items; or (b) items covered by Category I(h) of the USML solely by reference to Category I(a), excluding Military Equipment. Military Equipment means (1) Drum and other magazines for firearms to .50 caliber (12.7 mm) inclusive with a capacity greater than 50 rounds, regardless of jurisdiction of the firearm, and specially designed parts and components therefor; (2) Parts and components specially designed for conversion of a semi-automatic firearm to a fully automatic firearm; (3) Accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting, and specially designed parts and components therefor.

This temporary modification will remain in effect while the final rule referenced in paragraph 1(a) of the Settlement Agreement is in development.

Please see the Settlement Agreement [insert relevant hyperlink] and the Second Amended Complaint [insert relevant hyperlink] for additional information.



United States Department of State
Bureau of Political-Military Affairs
Directorate of Defense Trade Controls
Washington, D.C. 20522-0112

Cody R. Wilson, Defense Distributed, and Second Amendment Foundation, Inc.
c/o Matthew A. Goldstein
Matthew A. Goldstein, PLLC
1875 Connecticut Ave NW, 10th Floor
Washington, DC 20009

RE: Directorate of Defense Trade Controls Approval of Certain Files for Public Release

Dear Mr. Wilson, Defense Distributed, and Second Amendment Foundation, Inc.:

This letter is provided in accordance with section 1(c) of the Settlement Agreement in the matter of *Defense Distributed, et al., v. U.S. Department of State, et al.*, No. 15-cv-372-RP (W.D. Tx.) (hereinafter referred to as “*Defense Distributed*”). As used in this letter,

- The phrase “Published Files” means the files described in paragraph 25 of Plaintiffs’ Second Amended Complaint in *Defense Distributed*.
- The phrase “Ghost Gunner Files” means the files described in paragraph 36 of Plaintiffs’ Second Amended Complaint in *Defense Distributed*.
- The phrase “CAD Files” means the files described in paragraph 40 of Plaintiffs’ Second Amended Complaint in *Defense Distributed*.

The Department understands that Defense Distributed submitted the Published Files, Ghost Gunner Files, and CAD Files to the Department of Defense’s Defense Office of Prepublication and Security Review (DOPSR) in 2014 to request review for approval for public release pursuant to International Traffic in Arms Regulations (ITAR) § 125.4(b)(13). It is our further understanding that DOPSR did not make a determination on the eligibility of these files for release, but instead referred you to the Directorate of Defense Trade Controls (DDTC) regarding public release of these files.

I advise you that for the purposes of International Traffic in Arms Regulations (ITAR) § 125.4(b)(13), the Department of State is a cognizant U.S. government department or agency, and DDTC has authority to issue the requisite approval for public release. To that end, I approve the Published Files, Ghost Gunner Files, and CAD Files for public release (i.e., unlimited distribution). As set forth in ITAR §125.4(b)(13), technical data approved for public release by the cognizant U.S. government department or agency is not subject to the licensing requirements of the ITAR.

Sincerely,

Acting Deputy Assistant Secretary for the
Directorate of Defense Trade Controls

SETTLEMENT AGREEMENT

Defense Distributed (“DD”), Second Amendment Foundation, Inc. (“SAF”), and Conn Williamson (collectively, “Plaintiffs,”) and the United States Department of State (“State”), the Secretary of State, the Directorate of Defense Trade Controls (“DDTC”), the Deputy Assistant Secretary, Defense Trade Controls, and the Director, Office of Defense Trade Controls Policy (collectively, “Defendants”), out of a mutual desire to resolve all of the claims in the case captioned *Defense Distributed, et al. v. Dep’t of State, et al.*, Case No. 15-cv-372-RP (W.D. Tex.) (the “Action”) without the need for further litigation and without any admission of liability, hereby stipulate and agree as follows:

Plaintiffs and Defendants do hereby settle all claims, issues, complaints, or actions described in the case captioned, and any and all other claims, complaints, or issues that have been or could have been asserted by Plaintiffs against Defendants in accordance with the following terms and conditions:

1. *Consideration:* In consideration of Plaintiffs’ agreement to dismiss the claims in the Action with prejudice as described in paragraph 2, below, Defendants agree to the following, in accordance with the definitions set forth in paragraph 12, below:

- (a) Defendants’ commitment to draft and to fully pursue, to the extent authorized by law (including the Administrative Procedure Act), the publication in the Federal Register of a notice of proposed rulemaking and final rule, revising USML Category I to exclude the technical data that is the subject of the Action.
- (b) Defendants’ announcement, while the above-referenced final rule is in development, of a temporary modification, consistent with the International

Traffic in Arms Regulations (ITAR), 22 C.F.R. § 126.2, of USML Category I to exclude the technical data that is the subject of the Action. The announcement will appear on the DDTC website, www.pmdtc.state.gov, on or before July 27, 2018.

- (c) Defendants' issuance of a letter to Plaintiffs on or before July 27, 2018, signed by the Deputy Assistant Secretary for Defense Trade Controls, advising that the Published Files, Ghost Gunner Files, and CAD Files are approved for public release (i.e., unlimited distribution) in any form and are exempt from the export licensing requirements of the ITAR because they satisfy the criteria of 22 C.F.R. § 125.4(b)(13). For the purposes of 22 C.F.R. § 125.4(b)(13) the Department of State is the cognizant U.S. Government department or agency, and the Directorate of Defense Trade Controls has delegated authority to issue this approval.
- (d) Defendants' acknowledgment and agreement that the temporary modification of USML Category I permits any United States person, to include DD's customers and SAF's members, to access, discuss, use, reproduce, or otherwise benefit from the technical data that is the subject of the Action, and that the letter to Plaintiffs permits any such person to access, discuss, use, reproduce or otherwise benefit from the Published Files, Ghost Gunner Files, and CAD Files.
- (e) Payment in the amount of \$39,581.00. This figure is inclusive of any interest and is the only payment that will be made to Plaintiffs or their counsel by Defendants under this Settlement Agreement. Plaintiffs' counsel will provide Defendants'

counsel with all information necessary to effectuate this payment.

The items set forth in subparagraphs (a) through (e) above constitute all relief to be provided in settlement of the Action, including all damages or other monetary relief, equitable relief, declaratory relief, or relief of any form, including but not limited to, attorneys' fees, costs, and/or relief recoverable pursuant to 2 U.S.C. § 1302, 2 U.S.C. § 1311, 2 U.S.C. § 1317, 22 U.S.C. § 6432b(g), 28 U.S.C. § 1920, Fed. R. Civ. P. 54(d), and the Local Rules.

2. *Dismissal with Prejudice:* At the time of the execution of this Settlement Agreement, Plaintiffs agree to have their counsel execute and provide to Defendants' counsel an original Stipulation for Dismissal with Prejudice pursuant to Fed. R. Civ. P. 41(a)(1)(A)(ii) and 41(a)(1)(B). Counsel for Defendants agree to execute the stipulation and file it with the Court in the Action, no sooner than 5 business days after the publication of the announcement described in Paragraph 1(b) of this Settlement Agreement and issuance of the letter described in Paragraph 1(c) of this Settlement Agreement. A copy of the Stipulation for Dismissal with Prejudice is attached hereto.
3. *Release:* Plaintiffs, for themselves and their administrators, heirs, representatives, successors, or assigns, hereby waive, release and forever discharge Defendants, and all of their components, offices or establishments, and any officers, employees, agents, or successors of any such components, offices or establishments, either in their official or

individual capacities, from any and all claims, demands and causes of action of every kind, nature or description, whether currently known or unknown, which Plaintiffs may have had, may now have, or may hereafter discover that were or could have been raised in the Action.

4. *No Admission of Liability:* This Settlement Agreement is not and shall not be construed as an admission by Defendants of the truth of any allegation or the validity of any claim asserted in the Action, or of Defendants' liability therein. Nor is it a concession or an admission of any fault or omission in any act or failure to act. Nor is it a concession or admission as to whether the monetary or equitable relief, attorneys' fees, costs, and expenses sought by Plaintiffs in the Action, are reasonable or appropriate. None of the terms of the Settlement Agreement may be offered or received in evidence or in any way referred to in any civil, criminal, or administrative action other than proceedings permitted by law, if any, that may be necessary to consummate or enforce this Settlement Agreement. The terms of this Settlement Agreement shall not be construed as an admission by Defendants that the consideration to be given hereunder represents the relief that could be recovered after trial. Defendants deny that they engaged in *ultra vires* actions, deny that they violated the First Amendment, Second Amendment, or Fifth Amendment of the United States Constitution, and maintain that all of the actions taken by Defendants with respect to Plaintiffs comply fully with the law, including the United States Constitution.

5. *Merger Clause:* The terms of this Settlement Agreement constitute the entire agreement of Plaintiffs and Defendants entered into in good faith, and no statement, remark, agreement or understanding, oral or written, which is not contained therein, shall be recognized or enforced. Plaintiffs acknowledge and agree that no promise or representation not contained in this Settlement Agreement has been made to them and they acknowledge and represent that this Settlement Agreement contains the entire understanding between Plaintiffs and Defendants and contains all terms and conditions pertaining to the compromise and settlement of the disputes referenced herein. Nor does the Parties' agreement to this Settlement Agreement reflect any agreed-upon purpose other than the desire of the Parties to reach a full and final conclusion of the Action, and to resolve the Action without the time and expense of further litigation.
6. *Amendments:* This Settlement Agreement cannot be modified or amended except by an instrument in writing, agreed to and signed by the Parties, nor shall any provision hereof be waived other than by a written waiver, signed by the Parties.
7. *Binding Successors:* This Settlement Agreement shall be binding upon and inure to the benefit of Plaintiffs and Defendants, and their respective heirs, executors, successors, assigns and personal representatives, including any persons, entities, departments or agencies succeeding to the interests or obligations of the Parties.

8. *Consultation with Counsel:* Plaintiffs acknowledges that they have discussed this Settlement Agreement with their counsel, who has explained these documents to them and that they understand all of the terms and conditions of this Settlement Agreement. Plaintiffs further acknowledge that they have read this Settlement Agreement, understand the contents thereof, and execute this Settlement Agreement of their own free act and deed. The undersigned represent that they are fully authorized to enter into this Settlement Agreement.
9. *Execution:* This Settlement Agreement may be executed in one or more counterparts, each of which shall be deemed an original, and all of which together constitute one and the same instrument, and photographic copies of such signed counterparts may be used in lieu of the original.
10. *Jointly Drafted Agreement:* This Settlement Agreement shall be considered a jointly drafted agreement and shall not be construed against any party as the drafter.
11. *Tax and Other Consequences:* Compliance with all applicable federal, state, and local tax requirements shall be the sole responsibility of Plaintiffs and their counsel. Plaintiffs and Defendants agree that nothing in this Settlement Agreement waives or modifies federal, state, or local law pertaining to taxes, offsets, levies, and liens that may apply to this

Settlement Agreement or the settlement proceeds, and that Plaintiffs are executing this Settlement Agreement without reliance on any representation by Defendants as to the application of any such law.

12. *Definitions:* As used in this Settlement Agreement, certain terms are defined as follows:

- The phrase “*Published Files*” means the files described in paragraph 25 of Plaintiffs’ Second Amended Complaint.
- The phrase “*Ghost Gunner Files*” means the files described in paragraph 36 of Plaintiffs’ Second Amended Complaint.
- The phrase “*CAD Files*” means the files described in paragraph 40 of Plaintiffs’ Second Amended Complaint.
- The phrase “*Other Files*” means the files described in paragraphs 44-45 of Plaintiffs’ Second Amended Complaint.
- The phrase “*Military Equipment*” means (1) Drum and other magazines for firearms to .50 caliber (12.7 mm) inclusive with a capacity greater than 50 rounds, regardless of jurisdiction of the firearm, and specially designed parts and components therefor; (2) Parts and components specially designed for conversion of a semi-automatic firearm to a fully automatic firearm; (3) Accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting, and specially designed parts and components therefor.
- The phrase “*technical data that is the subject of the Action*” means: (1) the Published Files; (2) the Ghost Gunner Files; (3) the CAD Files; and (4) the Other Files insofar as those files regard items exclusively: (a) in Category I(a) of the United States Munitions List (USML), as well as barrels and receivers covered by Category I(g) of the USML that are components of such items; or (b) items

covered by Category I(h) of the USML solely by reference to Category I(a),
excluding Military Equipment.

Dated: _____, 2018

Dated: June 29, 2018



Matthew A. Goldstein
Snell & Wilmer LLP
One South Church Ave. Ste. 1500
Tucson, Arizona 85701
Counsel for Plaintiffs

Dated: _____, 2018

Eric J. Soskin
Stuart J. Robinson
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W.
Washington, D.C. 20001
Tel. (202) 353-0533

Counsel for Defendants

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, et al.,
Plaintiffs,

v.

U.S. DEPARTMENT OF STATE, et al.,
Defendants.

§
§
§
§
§
§
§

No. 1:15-cv-372-RP

STIPULATION OF DISMISSAL WITH PREJUDICE

Pursuant to Federal Rule of Civil Procedure 41(a)(1)(A)(ii) and 41(a)(1)(B), and a settlement agreement among Plaintiffs (Defense Distributed, Second Amendment Foundation, Inc., and Conn Williamson) and Defendants (the United States Department of State, the Secretary of State, the Directorate of Defense Trade Controls, the Deputy Assistant Secretary, Defense Trade Controls, and the Director, Office of Defense Trade Controls Policy), the Plaintiffs and the Defendants hereby stipulate to the dismissal with prejudice of this action.

Dated: June 29, 2018

Respectfully submitted,



Matthew Goldstein
D.C. Bar No. 975000*
Snell & Wilmer LLP
One South Church Ave., Ste. 1500
Tucson, Arizona 85701
520.882.1248 / Fax 520.884.1294
mgoldstein@swlaw.com

CHAD A. READLER
Acting Assistant Attorney General
Civil Division

ANTHONY J. COPPOLINO
Deputy Branch Director
Federal Programs Branch

Alan Gura
Virginia Bar No. 68842*
Gura PLLC
916 Prince Street, Suite 107
Alexandria, Virginia 22314

ERIC J. SOSKIN
Pennsylvania Bar No. 200663
Senior Trial Counsel

703.835.9085/Fax 703.997.7665

alan@gurapllc.com

William T. "Tommy" Jacks

Texas State Bar No. 10452000

David S. Morris

Texas State Bar No. 24032877

FISH & RICHARDSON P.C.

111 Congress Avenue, Suite 810

Austin, Texas 78701

512.472.5070 / Fax 512.320.8935

jacks@fr.com

dmorris@fr.com

Josh Blackman

Virginia Bar No. 78292

1303 San Jacinto Street

Houston, Texas 77002

202.294.9003/Fax: 713.646.1766

joshblackman@gmail.com

Attorneys for Plaintiffs

*Admitted pro hac vice

STUART J. ROBINSON

California Bar No. 267183

Trial Attorney

United States Department of Justice

Civil Division, Federal Programs Branch

20 Massachusetts Ave., NW, Room 7116

Washington, DC 20530

Phone: (202) 514-1500

Fax: (202) 616-8470

Email: Eric.Soskin@usdoj.gov

Attorneys for Defendants